OFFICE OF LEGAL SERVICES 11-1000

Legal Assistance Requests 11-1010

Department employees may seek legal advice or consultation, regarding ongoing department business, directly from Office of Legal Services (OLS) attorneys assigned to the employee's Center, Office or Division. However, requests for formal written legal opinions should be submitted through the Deputy Director to the Chief Counsel, OLS. Contacts with OLS should be only from department employees who are so authorized by their chain of command. Requests for legal opinions or advice should normally be considered as confidential and comply with the guidelines on attorney-client privilege and attorney's work product set forth below in Chapter 11-1020.

Privileged Communications and Attorney's Work Product 11-1020

Communications of legal opinions and advice, either verbally or in writing, to persons outside of the Department are prohibited without the specific authorization of OLS. Distribution of documents, including e-mail, containing legal opinions and advice within the Department shall be limited to persons on a strict need-to-know basis and shall not be reproduced, circulated, nor forwarded to anyone other than the original recipients to whom OLS initially sent the opinion. Other circulation or reproduction is not permitted without advance approval from OLS.

Use attorneys within OLS, or outside counsel specifically authorized by OLS, to obtain facts in anticipation of litigation, rather than routing requests or information from program staff through normal department channels. If non- lawyers are used to gather facts, their reports shall be clearly identified as having been prepared at the request of legal counsel, and all related materials should be delivered to counsel (e.g., drafts, questionnaires, interview memoranda).

Allow counsel an opportunity to carefully review the contents of investigative or analytical reports where there is a possibility of litigation. Reports that are generated because of an existing lawsuit, a pending or imminent Department investigation or other proceeding, or an anticipated claim should set forth that purpose in the introduction. If non-attorneys are operating with instructions from and pursuant to the supervision of counsel, that fact should be explicitly stated at or very near the beginning of any such reports.

When an attorney in OLS (or other legal counsel authorized by OLS) requests data, information, or an investigation from you, address your response to the attorney, preferably with a preface that the document is in response to his or her request. Do not have your response copied to any other non-attorney. Copies of such responses should be maintained in segregated files. Whenever possible, have the response sent directly to the attorney, rather than through your supervisor or some other intermediary.

Litigation Holds 11-1025

Employees must follow document retention policies and destroy old or unnecessary documents in accordance with those policies. However, when the Department reasonably

anticipates it may be involved in litigation, whether as a party or as a nonparty in possession of relevant evidence, it has a legal obligation to suspend its routine document retention policies and institute a written litigation hold to ensure relevant documents are not destroyed. As soon as possible after determining that a litigation hold is necessary, OLS shall draft a litigation hold notice and disseminate it to all Department staff who are likely to possess potentially relevant evidence. OLS will work directly with information technology staff and the custodians of records to implement the litigation hold.

The Information Security Office (ISO) will follow designed procedures for preserving the organization and integrity of files and perform special file searches, when an investigation is begun, or litigation is imminent. ISO will preserve and record all file source information for documents subject to claims of privilege or work product in connection with file searches, whether voluntary or pursuant to legal process. This information will be necessary to establish confidentiality. ISO will include information regarding the location where the files were kept and who had access to those files, in addition to the information on routine file identification.

Subpoenas 11-1030

Subpoenas can be addressed to the Department or its programs, or to individual employees. A subpoena may be addressed to the Department, to a Department "Person Most Knowledgeable," to a Department "Custodian of Records," or to a named employee. Depending on to whom the subpoena is addressed, OLS may or may not be the proper entity to accept service. It is very important to carefully read the subpoena to determine to whom it is addressed in order to determine who is authorized to accept service.

OLS is the preferred entity to accept service of a subpoena addressed to the Department; a Department "Person Most Knowledgeable"; a Department "Custodian of Records"; and a Department official named in his or her official capacity. However, a District Office or the Richmond Campus may accept service of such subpoenas; please coordinate with OLS to ensure proper review of the subpoena before acceptance of service. Process servers attempting to serve such subpoenas upon an office other than OLS, a District Office, or the Richmond Campus should be directed to serve OLS at:

1415 L Street
Sacramento, CA 95814

Subpoenas addressed to a named employee must be accepted by the named employee or their supervisor. A subpoena naming Department staff in their personal capacities will not be accepted by OLS unless specifically authorized by the named individual. Service of a subpoena upon an employee named in his or her personal capacity must be made only upon that person, and other employees should not accept service on that person's behalf.

Before a subpoena is accepted through personal service, it should be examined to make sure that it is valid. A subpoena must be addressed to the Department or an individual as indicated above. It must seek records or testimony pursuant to litigation and give at least ten (10) days to respond. A subpoena must include payment of copy fees or witness fees. The check must be sent to Accounting along with the Index Code, PCA and object code 414 for each subpoenaed employee. A subpoena for records of an individual must include

proof of service of a Notice to Consumer that was served on the individual whose records are sought.

Subpoenas must be personally served unless the process server has prior approval to serve the Department by fax, email or mail. If a subpoena is received by fax, email or mail without prior approval, staff should forward it to OLS for handling. If a subpoena is drop-served (personally served without giving staff the opportunity to review the subpoena), the subpoena should be reviewed to ensure it meets the above requirements. If it does not, staff should forward it to OLS for handling.

After accepting a subpoena, staff should contact OLS if the subpoena is: a) from the Workers Compensation Appeals Board and the named employer is CDPH; b) requesting records from the Office of AIDS or c) if staff does not think records can be released or appearance made due to privacy protections.

Summons and Complaints, Writs, Etc. 11-1040

A summons and complaint, or a summons and petition for writ of mandate, is the package of legal material that is served to commence a lawsuit. Process servers may attempt to serve such papers on (1) the Department, its Director, its officers, or its employees, where they are named in their official capacities; and (2) individual CDPH employees named in their personal capacity.

OLS is the only entity that should accept service of such papers on behalf of the Department, its Director, its officers, or its employees, where they are named in their official capacities. Staff members, other than OLS staff members, should not accept service of such papers. Instead, process servers attempting to serve such papers should be directed to serve OLS at:

1415 L Street
Sacramento, CA 95814

A summons and complaint naming individual department staff in their personal capacities cannot be accepted for service by OLS. Service of a summons and complaint upon a defendant named in his or her personal capacity must be made only upon that person, and other employees should not accept service on that person's behalf.
If a summons and complaint are served by mail upon an office other than OLS, the entire original package, along with the original envelope, must immediately be delivered by hand, or sent by overnight mail, to OLS. If sent by mail, the sender should make a copy of the entire package served and alert OLS by telephone or e-mail that the original is being sent. The Acknowledgement of Service by Mail form should not be completed but should be forwarded to OLS along with the rest of the summons and complaint package.

Contacts With the Office of the Attorney General 11-1050

Except as specifically directed and authorized by OLS, department staff should not contact the Office of the Attorney General on matters involving department business. If contacted by a member of the Office of the Attorney General on a matter involving department business, department staff are to refer the call to OLS.

Contacts With Private Attorneys 11-1060

Whenever departmental staff anticipate meeting with any attorney regarding departmental business, OLS must be contacted in advance so it can be determined whether representation or involvement by one of the Department's attorneys is necessary or desirable. Department staff should advise OLS about any verbal or written communication with a private attorney concerning department business prior to responding to such inquiries. Consulting with outside legal counsel on departmental issues or programs, whether in a paid or pro bono capacity, must be approved by the Chief Counsel.

EMPLOYEE CONDUCT 11-2000

Conflict of Interest Code 11-2010

The Political Reform Act of 1974 (Government Code, Title 9, section 81000 *et seq*.; Act) prohibits **all** state employees from participating in governmental decisions that may materially affect their financial interests.

The Act also requires designated employees to file a Statement of Economic Interest (Form 700) whereby financial interests are reportable pursuant to disclosure categories. The Form 700 must be filed within 30 days of appointment to a designated position with CDPH; annually thereafter (by April 1 of each year); and within 30 days of leaving a designated position. Each state agency adopts a Conflict of Interest (COI) Code under the authority of the Political Reform Act, which identifies designated employees and disclosure categories.

The Department's COI Code is located at California Code of Regulations, Title 22, section 20100.5 (including Appendices A and B). Appendix A designates the classifications, contractors, and advisory committee members (designated reporters) who must file a Form 700 and lists their respective required disclosure category/ies. Appendix B specifies what financial interests must be reported pursuant to each disclosure category. Each Department employee shall review Appendix A to determine whether their classification is listed as a designated reporter and, if so, what disclosure categories are reportable on their Form 700. The employee should then review the details of each disclosure category listed in Appendix B to determine any financial interests that must be reported pursuant to the details of applicable disclosure category/ies.

Objectives 11-2020

The goals of the Department's COI Code mirror those of the Political Reform Act: State government should serve the needs and respond to the wishes of all citizens without regard to their wealth. Public officials should perform their duties in an impartial manner, free from bias caused by their own financial interests or the financial interests of persons who have supported them. Public officials are required to disclose assets and income that may be materially affected by their official actions. In some instances, public officials should be disqualified from acting to avoid conflicts of interest.

Resources related to the Department's COI Code and other COI information and links are located on the Conflict of Interest and Ethics Training Resource Page on the Department's intranet.

Responsibilities **11-2030**

Human Resources Division **11-2031**

The Employee Relations and Resource Branch Chief, within the Human Resources Division, is the designated Filing Officer for the Department, and oversees the Department's compliance with the provisions of the Political Reform Act (Government Code sections 81010 and 82027; Cal. Code Regs., tit. 2, section 18115). Significant (but not all-inclusive) responsibilities of the Filing Officer are:

1. Issuing forms for annual filing of Statements of Economic Interest (Fair Political Practices Commission "FPPC", Form 700) to every employee in a designated position, assuring employees' compliance, and maintaining the Department's file of same. Forms can be issued via e-mail attachments or by providing the link to where the forms and instructions can be completed electronically via the eDisclosure web site for the FPPC. Such e-mail notices can be sent to all staff of the Department, indicating that it is only for those who are designated to file a Form 700.

2. Informing employees moving into or leaving designated positions of the need to file an "assuming office" or "leaving office" Form 700.

3. Determining from appropriate Chief Deputy Director/Deputy Directors whether reclassified designated positions require a change in COI disclosure categories.

4. Identifying proposed designations and category changes and contacting OLS regarding the need to amend the COI Code.

5. Work with the OLS to prepare and submit a regulatory package to the FPPC for approval.

Division Chiefs and Above **11-2032**

Responsibilities of Chief Deputy Directors, Deputy Directors, Center/Office Directors, and Division Chiefs relating to the COI Code include the following:

1. Advising the Filing Officer (Employee Relations and Resource Branch Chief within the Human Resources Division) when newly created positions meet the filing criteria of the Department's COI Code or Political Reform Act, specifying the disclosure categories under which these positions would file yearly Form 700, and providing the Filing Officer with duty statements for the positions which describe the specific responsibilities that qualify them as designated positions.

2. Notifying the Filing Officer when changes in responsibilities of designated

positions require changes in disclosure categories and identifying the new categories under which the positions would file yearly Form 700.

3. Ensuring that a contractor is designated to file a Form 700 if that individual performs substantially the same duties as a Department office or job classification that is required to file a Form 700 (see Consultants/Contractors 11-2045).

Ensuring that any advisory committee under their jurisdiction has been reviewed by OLS for potential designation as requiring a Form 700 from each member, and if so-designated, ensuring that all members file a Form 700 and that the roster of members and their completed Form 700s are submitted to the Human Resources Division for filing.

Incompatible Activities **11-2040**

Intent of Law **11-2041**

Section 19990 of the Government Code requires the Department to adopt a statement of those activities that are inconsistent, incompatible, in conflict with, or inimical to the duties of employees of the Department. This chapter 11-2040 constitutes that statement.

In this statement, the Department has set forth activities that are absolutely prohibited and activities that require an individual determination as to whether they are inconsistent, incompatible, in conflict with, or inimical to duties. The Department affirms its intent to review on a case-by-case basis each activity in the second group when such review is requested by the affected employee. In the absence of such a request and a review in accordance with the procedure established by this statement, the activity will be deemed inconsistent, incompatible, in conflict with, or inimical to duties, and the employee engaging in the activity will be subject to disciplinary action up to and including termination as outlined in Government Code section19572(r).

Definitions **11-2042**

“Employee” includes any officer or employee of the Department, as defined in Government Code section 19815(d). This definition of “employee” applies throughout this statement.

“Person” includes individuals, firms, corporations, partnerships, associations, other governmental bodies, or agents and representatives of these persons. This definition of “person” applies throughout this statement.

“Outside employment” is defined as any services performed by a department employee on his or her own time, during other than normal working hours, for which he or she may receive any form of compensation that, over 12 months, equals or exceeds the income amount listed in Government Code section 87103.

Prohibited Activities **11-2043**

The following activities of employees of the Department are hereby declared to be

inconsistent, incompatible, in conflict with, or inimical to duties and as such are prohibited:

1. No employee shall provide a service for salary, honorarium, or compensation of any nature so that the employee is receiving dual compensation from the State and from another source for the same period of time, such as during work hours. This does not apply to employees while they are on vacation, compensating time off, or military leave.

2. No employee shall receive or accept money or any other consideration from anyone other than the State for the performance of an act that the employee would be required or expected to render in the regular course of hours of their state employment or as part of their duties as an officer or employee of the Department.

3. No employee shall claim travel expenses from the State for other than State business. No employee shall accept dual payment for travel expenses.

4. No employee shall receive any gratuity or gifts (including meals, lodging, services, entertainment, travel expenses, or any other thing of value) equaling or exceeding the amount allowed by Government Code section 87103 or any regulations promulgated pursuant to that statute over a 12-month period from any person, organization, firm, or corporation, including parents, subsidiaries, agents, or committees, that is (1) subject to regulation, inspection, supervision, licensing, certification, or audit by the Department or any local agency under the supervision of the Department, or that (2) has financial dealings with the Department or any local agency under the supervision of the Department. No employee shall claim reimbursement from the Department for meals, lodging, or travel expenses where provided by others as gifts. The term “gift” is defined in accordance with Government Code section 82028.

5. Favors are to be refused. An employee is to advise their supervisor immediately of any attempt by nonemployees to influence favorable action by the State. All gifts received in excess of the above-established limits are to be returned. The return of these gifts can be at the expense of the Department, through its mailroom, and can include any insurance needed. Perishables of value shall be given to a charity, and the person who sent the gifts shall be informed of this action. No state or federal tax deduction shall be claimed for donations to a charity.

6. No employee shall in any way use their official position for personal gain.

7. No employee shall use departmental records for private gain, and no employee shall divulge confidential departmental information unless officially authorized to do so. This includes divulging information, data, or intelligence from departmental reports, records, correspondence, or manuals when the release of such has not been authorized.

8. No employee shall engage in any act knowing that the act or conduct outside of their employment with the Department may later be subject (directly or indirectly) to the Department’s enforcement authority, including its authority to regulate, inspect,

review, audit or control the conduct.

9. No employee shall engage in conduct that may negatively impact their ability to perform their job or detract from the Department's mission.

10. No employee shall use during or outside of office hours, any Department symbol, badge, identification card, record, information, facilities, staff time, equipment, supplies, training material, vehicle, telephone, addresses, postage, mailing lists, or influence of state position for personal gain or advantage, nor lend such items to clients, contractors, providers, or other persons, unless authorized by law.

11. No employee shall initiate contact with state administrative or legislative personnel for the purpose of presenting the Department's policy or position on legislation or amendments thereto or initiative or referendum petitions, unless such act is a part of the employee's official duty. This section shall not be interpreted to preclude employees, as private citizens, from contacting legislative or administrative personnel.

12. No employee shall engage in partisan political activity that is prohibited by the federal Hatch Act or applicable state statutes. It is the duty of each employee to become familiar with permitted and prohibited activities under federal and state law Title 5 United States Code section 1501 et seq. and California Government Code section 3201 et seq.)

13. No employee shall engage in any outside employment, activity, or enterprise that involves such a time demand that it results in less efficient or impaired performance of the employee's regular state duties.

Outside Employment **11-2044**

1. A departmental employee who wishes to engage in outside employment or an activity that is directly or indirectly related to the functions and responsibilities of their program or division must first receive a written determination from their supervisor that such outside employment or activity is not inconsistent, incompatible, in conflict with, or inimical to the employee's duties to the Department. The employee's supervisor shall communicate their decision in writing within five business days of the receipt of the request for determination.

2. Subsections a through e, below, list some of those types of outside employment or activity that, when engaged in by an employee, require a written determination by the employee's supervisor as to whether the outside employment or activity is inconsistent, incompatible, in conflict with, or inimical to the employee's duties to the Department. (See Government Code section 19990 for more categories.) It is the employee's responsibility to seek a written determination in the manner set forth in number 1 above. If the employee fails to seek a written determination, the outside employment or activity is automatically deemed inconsistent, incompatible, in conflict with, or inimical to their duties to the Department.

   A written determination must be sought in regard to the following types of outside

employment or activity:

a. Outside employment for an organization that is supported by funds approved or administered by the employee's center or division.

b. Provision of consultation or service by an employee licensed in one of the healing arts to any patient, resident, or client of a facility or program licensed by the Department.

c. Acting as private consultant for any person to whom the Department, or any local agency under the supervision of the Department, refers patients.

d. Owning or being a partner in or acting as an officer or board member of, or as a consultant or contractor to, or having any financial interest in any business institution or any agency that (1) the employee knows, or suspects is subject to regulation, inspection, supervision, licensing, certification, or audit by the Department or by any local agency under the supervision of the Department or that (2) has financial dealings with the Department. Such businesses include, but are not limited to, skilled-nursing facilities, residential and intermediate care homes, hospitals, ambulance services, drug stores, pharmacies, clinics, and clinical laboratories.

e. Outside employment with any person or entity that is subject to regulation, inspection, supervision, licensing, certification, investigation, or audit by the Department when such employment is to be substantially similar or related to the employee's position or function with the Department, shall first seek determination of compatibility from their supervisor.

f. Regarding the provision of outside legal services, attorneys are subject to (e) above and must obtain a determination by their supervisors that any outside legal services are not incompatible with their duties for the Department.

3. If the supervisor notifies an employee in writing within the specified time that it has been determined that the desired outside employment or activity is inconsistent, incompatible, in conflict with, or inimical to the employee's duties to the Department, the employee may appeal through the grievance procedure as prescribed by their Bargaining Unit's Memorandum of Understanding.

Consultants/Contractors **11-2045**

A consultant or contractor is generally covered by the Political Reform Act, conflict of interest laws, Statement of Economic Interest–filing requirements, and related requirements to the same extent as for similarly situated employees of the Department performing the same or similar duties as the consultant or contract employee. Departmental employees who are responsible for monitoring such contracts are responsible both for advising consultants and contractors of these responsibilities and for ensuring compliance, including, but not limited to, the potential need for such consultant or contractor to file a Form 700, Statement of Economic Interest.

Conflict of Interest: Provisions of Public Contract Code 11-2050

The Public Contract Code contains various provisions that prohibit current and former state employees from engaging in certain activities. The law provides that any contracts entered into in violation of these provisions are void. (Public Contract Code section 10420.)

Public Contract Code 10410: Prohibition Against Current State Employees Contracting as an Independent Contractor 11-2051

The Public Contract Code prohibits all current state employees from contracting on his or her own behalf with any state agency. The law states: “No officer or employee in the state civil service shall contract on his or her own individual behalf as an independent contractor with any state agency to provide services or goods.” (Public Contract Code section 10410.)

Public Contract Code 10410: Prohibition Against Current State Employees Being Compensated for Any Activity That Is Funded by the State Except as a Condition of Regular Employment 11-2052

The Public Contract Code also prohibits current state employees from engaging in any activity that is sponsored or funded by any state contract and from which the employee receives any compensation or in which the employee has a financial interest unless the activity is required as a part of the employee’s regular state employment. That law states: “No officer or employee in the state civil service or other appointed state official shall engage in any employment, activity, or enterprise from which the officer or employee receives compensation or in which the officer or employee has a financial interest and which is sponsored or funded, or sponsored and funded, by any state agency or department through or by a state contract unless the employment, activity, or enterprise is required as a condition of the officer's or employee's regular state employment.” (Public Contract Code section 10410.)

Public Contract Code 10411: Time Prohibition Retired, Dismissed, Separated, or Former State Employees 11-2053

Additional provisions of the Public Contract Code apply to former state employees. One section of the law prohibits former employees for two years from entering into any contracts in which the employee was involved while employed by the State. The law states: “No retired, dismissed, separated, or formerly employed person of any state agency or department employed under the state civil service or otherwise appointed to serve in state government may enter into a contract in which he or she engaged in any of the negotiations, transactions, planning, arrangements, or any part of the decision making process relevant to the contract while employed in any capacity by any state agency or department. The prohibition of this subdivision shall apply to a person only during the two-year period beginning on the date the person left state employment.” (Public Contract Code section 10411(a).)

Another section of the law prohibits former employees for one year from contracting with the former state agency if the employee had a policymaking position in the general area covered by the contract. That law states:

> For a period of 12 months following the date of his or her retirement, dismissal, or separation from state service, no person employed under State civil service or otherwise appointed to serve in state government may enter into a contract with any state agency, if he or she was employed by that state agency in a policymaking position in the same general subject area as the proposed contract within the 12-month period prior to his or her retirement, dismissal, or separation. The prohibition of this subdivision shall not apply to a contract requiring the person's services as an expert witness in a civil case or to a contract for the continuation of an attorney's services on a matter he or she was involved with prior to leaving state service.

Public Contract Code section 10411(b).

Restriction on Participating in Governmental Decisions While Negotiating for Future Employment 11-2060

All officers, employees, or consultants of the Department are prohibited by law from participating in or using their official position to influence state agency decisions relating to persons with whom they are discussing future employment. The law provides: "No public official shall make, participate in making, or use their official position to influence, any governmental decision directly relating to any person with whom he or she is negotiating, or has any arrangement concerning, prospective employment." (Government Code section 87407.) For purposes of the preceding sentence, "public official" means every member, officer, employee, or consultant of a state or local agency. (See Government Code section 82048.)

Post-Employment Restrictions 11-2070

State law provides for restrictions on activities of former state officers and employees who engage in employment for compensation after leaving state service, in addition to those restrictions mentioned elsewhere in this manual. The law may be found in sections 87400 through 87410 of the Government Code.

Affected Persons 11-2071

The Political Reform Act applies to former state administrative officials. "State administrative official" means any member, officer, employee, or consultant of the Department who as part of their official responsibilities takes part personally in any particular matter involving a specific party or parties through decision, approval, disapproval, formal written recommendation, rendering advice on a substantial basis, investigation, or use of confidential information.

The law does not apply to former state administrative officials who participated in

particular matters in a purely clerical, secretarial, or ministerial capacity. These may include persons whose involvement in particular matters did not involve the exercise of independent discretion or judgment.

Prohibited Activities **11-2072**

No former state administrative official covered by the law after the termination of employment or term of office shall for compensation represent or aid, advise, counsel, consult, or assist in representing another party (except the State of California) before any court or state administrative agency or any officer or employee thereof if:

1. The State of California is a party or has a direct and substantial interest; and

2. The proceeding is one in which the former state administrative official participated.

"Represent" means to make any formal or informal appearance or to make any oral or written communication with the intent to influence a decision.

Government Code section 87403 provides for certain limited exceptions from the prohibited activities described above.

Violations **11-2073**

Violations concerning these prohibited activities are subject to the same civil, administrative, and criminal sanctions as those that may be imposed for enforcement of the Political Reform Act (Government Code section 81000 *et seq*.).

Use of State Time to Market Products **11-2074**

State and departmental policies prohibit employees' use of state time and resources to market products. In addition, departmental policies and the Incompatible Activities Statement prohibit employees from receiving dual compensation from the State and another source for the same period of time. (Ref. PHAM, Chapter 11, Legal, Section 11-2040.)

Definition of products includes, but is not limited to, cosmetics, housewares, mail orders, jewelry, and other sundry products.

Employees involved in the marketing of products must confine such activities to non-work hours.

Use or Possession of Alcohol or Substances on State Time **11-2075**

The following summary clarifies provisions of Government Code section 19572, Governor's Executive Order D-58-86, , and the Department's policy relative to alcohol and drug use on state time:

- Alcohol

  No state employee who is on duty or on standby for duty shall use or be under the influence of alcohol to the extent that it impairs the employee's ability to perform their duties safely and effectively. The consumption of alcohol on state property is prohibited.

- Illegal/Unauthorized Drugs/Substances

  No state employee who is on duty or on standby for duty shall use, possess, or be under the influence of illegal or unauthorized drugs or other illegal mind-altering substances.(See Title 2, California Code of Regulations, section 599.960.)

- Legally Prescribed Drugs

  Employees taking legally prescribed drugs that impair their ability to perform their duties safely and effectively may be temporarily relieved of those duties.

DELEGATION OF AUTHORITY 11-3000

Delegation 11-3010

Authority is officially delegated when an employee is empowered to personally represent the Director or take action on behalf of the Department in those matters specifically mandated to the Director.

Delegation Process 11-3020

Chief Executive Staff

1. The Director delegates full authority to the Chief Deputy Directors to act on behalf of the Department.

2. The Director's Office is responsible for maintaining and updating the delegation orders for the Chief Deputy Director.

Below Chief Executive Staff

1. Written delegation orders for positions below the Chief Deputy Director level are not required under Department policy.

2. A program may choose to maintain delegations of authority **below** the Chief Deputy Director or may modify position duty statements to include duties related to the delegation of authority.

   a. If a program chooses to maintain delegations below the Chief Deputy Director level, the program is responsible for developing the chain of delegation beginning from the Chief Deputy Director to the appropriate

program position level and for maintaining the delegation order system and procedures.

b. Modifying duty statements eliminates the need to process a new delegation order each time a change in staffing occurs. If a program chooses to modify a duty statement, the program will need to submit the duty statement with a Request for Personnel Action (RPA) to the Human Resources Division for review and filing.

INFORMATION PRIVACY PROGRAM 11-4000

Legal Mandate for Information Privacy Program 11-4010

Each state department and state agency shall enact and maintain a permanent privacy policy, in adherence with the Information Practices Act of 1977 (Title 1.8 (commencing with Section 1798) of Part 4 of Division 3 of the Civil Code)." (Government Code section 11019.9), including rules of conduct regarding personal information (Civil Code section 1798.20), a designated employee in charge of ensuring C/D/O compliance (Civil Code section 1798.22), and other guidelines, procedures, training, and compliance as outlined in the Information Practices Act (IPA) (Civil Code section 1798 et seq.) and the State Administrative Manual (SAM) (Sections 5100 and 5300.3). The California Department of Public Health will be referred to as (Department) in this Chapter:

Roles and Responsibilities

Executive Management: The Director has ultimate responsibility for information privacy within the Department. The Director is responsible and shall take reasonable measures for implementation of, and compliance with, the Department's privacy policy and is accountable for the information resources held by the Department. The Director is responsible for the integrity of information resources and the authorization of access to those resources. On an annual basis the Director must submit an Agency Designation Letter (SIMM section 5300 et. Seq.) designating critical personnel. (Select SAM section 5360). Each year the Director must certify that the agency is in compliance with state policy governing information technology security, risk management, and privacy program by submitting the Agency Risk Management and Privacy Program Compliance Certification (SIMM section 5300 et Seq.). (Select SAM sections 5305 and 5360.1).

Privacy Officer: The Privacy Officer provides legal analyses and policy recommendations to the Director and Executive Staff on federal and state laws, regulations, policies, and procedures related to the privacy of personal, confidential and sensitive information, including personal health information covered by the Health Insurance Portability and Accountability Act (HIPAA). The Privacy Officer develops and disseminates department privacy policies and procedures, based on an analysis of the laws in this area.

Chief Information Security Officer: The Department's Chief Information Security Officer (CISO) is vested with oversight responsibility at the department level for

ensuring the integrity and security of automated and paper files, databases, and computer systems. The CISO is required to oversee department compliance with policies and procedures regarding the security of information assets.

Technical Management: The Department's information technology management is responsible for: (1) implementing the necessary technical means to preserve the security, privacy, and integrity of the Department's information assets and manage the risks associated with those assets and (2) acting as a custodian of information per SAM section 5320.3.

Center/Division/Office (C/D/O): The Department's C/D/O managers are responsible: (1) for specifying and monitoring the integrity and security of information assets and the use of those assets within their areas of C/D/O responsibility and (2) for ensuring that C/D/O staff and other users of the information are informed of and carry out information security and privacy responsibilities.

Privacy Laws and Policies 11-4020

The following is a non-exhaustive discussion of privacy laws and policies that apply to the Department as well as a general summary of each law. Individual programs may have specific privacy laws with which they must comply. For questions, additional information, or more detail about any of these laws or policies, please contact the Privacy Office.

Article 1, Section 1 of the California Constitution establishes a right to privacy for all Californians. It specifically sets forth that pursuing and obtaining privacy is an inalienable right. A Californian's right to privacy, and the state's obligation to protect that right, is further outlined in the Information Practices Act of 1977 (IPA), which can be found at California Civil Code section 1798, et seq. The IPA places specific requirements on state agencies, including the Department, as to the collection, use, maintenance, and dissemination of information relating to individuals. It also defines the procedures the Department must follow for disclosing security incidents or breaches as well as the penalties for unauthorized disclosure of personally identifiable information. Another law, applicable to only a few of the Department's Programs, is the Health Insurance Portability and Accountability Act (HIPAA), which is Public Law No. 104-191. The HIPAA regulations, and specifically the HIPAA Privacy Rule, sets forth the specific procedures and requirements the Department must follow for handling certain healthcare information, and can be found at Title 45 of the Code of Federal Regulations section 160.101, et seq.

California Government Code section 11019.9 provides that state agencies are required to implement and post permanent privacy policies. The specifics around this law are laid out in state policy managed by the California Department of General Services, which can be found in the State Administrative Manual (SAM) section 5300 et seq. This section of the SAM also provides definitions, policies, and procedures for handling confidential, sensitive, personal, and public information. It also notes that every state department is responsible for the proper classification, use, and protection of its information technology. The California State Information Management Manual (SIMM), which is maintained by the California Department of Technology, also provides guidelines, procedures, and reports for information technology (IT) security and includes information on reporting IT security incidents and best practices for preventing such incidents.

Finally, as a public agency the Department is subject to The California Public Records Act (PRA). The PRA defines what records are open to public inspection, and therefore must be provided to individuals upon request, or are not open to public inspection and can be

withheld when requested. It requires departments to develop and implement procedures for the review of PRA requests and the release of public records in response to those requests.

Statement of Privacy Policy **11-4030**

Pursuant to Government Code section 11019.9, "Each state department . . . shall enact and maintain a permanent privacy policy, in adherence with the Information Practices Act of 1977. The permanent privacy policy of the California Department of Public Health will be referred as (Department) is as follows:

The Department is committed to promoting and protecting the privacy rights of individuals, as enumerated in Article 1 of the California Constitution, the Information Practices Act of 1977, and other state and federal laws.

It is the policy of the Department to limit the collection and safeguard the privacy of personal information collected or maintained by the Department. The Department's information management practices conform to the requirements of the Information Practices Act (Civil Code section 1798 et seq.), the Public Records Act (Government Code section 7920.000 et seq.), Government Code section 11019.9, and other applicable laws pertaining to information privacy.

It is the policy of the Department to adhere to the following principles in connection with the collection, creation, use and management of personal information:

- The Department collects personal information on individuals only as allowed by law.

- The Department limits the collection of personal information to what is relevant and necessary to accomplish a lawful purpose of the Department. Personal information, as defined in the Information Practices Act, includes, but is not limited to, information that identifies or describes an individual including, name, Social Security number (SSN), physical description, home address, home telephone number, education, financial matters, and medical or employment history.

- The Department endeavors in each instance to tell individuals who provide personal information to the Department the purpose for which the information is collected. The Department strives to tell individuals, who are asked to provide personal information, about the general uses that the Department will make of that information. The Department does this at the time of collection of the personal information.

- With each request for personal information, the Department provides information on the authority under which the request is made, the principal uses the Department intends to make of the information and the possible disclosures the Department is obligated to make to other government agencies and to the public.

- The Department provides individuals who provide personal information with an opportunity to review that information. The Department allows individuals, who provide personal information, to review the information and contest its accuracy or completeness.

- The Department uses personal information only for the specified purposes, or purposes consistent with those purposes, unless the Department obtains the consent of the subject of the information, or unless required or allowed by law or regulation.

- The Department uses information security safeguards. Regarding the personal information of individuals collected or maintained by the Department, the Department takes reasonable precautions to protect such information against loss, unauthorized access, and illegal use or disclosure.

- The Department's staff is trained on procedures for the management of personal information, including limitations on the disclosure of information. Access to personal information is limited to those members of the Department's staff whose work requires such access. Confidential information is destroyed according to the Department's records retention schedule. The Department conducts periodic reviews to ensure that proper information management policies and procedures are understood and followed.

- The general means by which personal data is protected by the Department against loss, unauthorized access, use modification or disclosure are posted in PHAM, Chapter 9, Information Technology, Section 9-1000 Information Security Policies and Chapter 11, Legal, Section 11-4000 Information Privacy Program.

- The Department will provide additional explanations of the Department's privacy policy, if requested. If any individuals have any further questions about the Department's privacy policy, they are encouraged to contact the Department's Privacy Office.

Health Insurance Portability and Accountability Act of 1996 (HIPAA) 11-4040

HIPAA-covered entities are responsible for designating the components that are part of one or more health care components of the covered entity . . . . " [45 CFR section 164.105(a)(2)(iii)(D)] The Department has determined that it is a "hybrid entity for purposes of application of the standards in the federal regulations entitled "Standards for Privacy of Individually Identifiable Health Information" (Privacy Rule} promulgated pursuant to the requirements of the Administrative Simplification subtitle of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The Privacy Rule governs the use and disclosure of protected health information.

Protected health information (PHI) is individually identifiable health information, which includes demographic information and is created or received by a Department HIPAA-covered health care component provider or health plan.

As a "hybrid entity" under HIPAA, the Department must have designated its "health care component" programs and services, including subdesignation of those components as either HIPAA "health plans" or "providers". (45 CFR section 164.505(a)(2)(iii)(D). As a hybrid entity under HIPAA, the Department as a whole is considered a HIPAA-covered entity whose business activities include both covered and noncovered functions. The Department has designated the following programs as HIPAA-covered health care components within CDPH performing covered functions:

Center for Family Health:
- Newborn Screening Program
- Prenatal Screening Program

Center for Infectious Disease
- AIDS Drug Assistance Program (ADAP)
- AIDS Medi-Cal Waiver Program (MCWP)
- ADAP Fiscal Forecasting, Evaluation, and Monitoring Section
- PrEP Assistance Program (PrEP AP)

Center for Healthy Communities
- California Gambling Education and Treatment Services Program (CalGETS)

All other department programs not listed above are considered by the Department to be non-HIPAA-covered components of the Department, performing noncovered functions, and thus not directly subject to HIPAA regulations.

Privacy Complaints 11-4050

1. Right to Complain Against Department-Scope of Complaints

   Individuals may make complaints concerning the Department's privacy policies and procedures or its compliance with such policies and procedures or the requirements of the Information Practices Act, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) or other state and federal privacy laws applicable to the Department.

2. Roles and Responsibilities

   Center/Division/Office (C/D/O) Managers: C/D/O managers will ensure their C/D/O comply with the following with respect to all privacy-related complaints received by or concerning their C/D/O:

   a. Create and maintain program specific procedures for the confidential receipt of complaints. When possible, request that complainants use the current Privacy Office CDPH 6242. Privacy/HIPAA Complaint.

   b. Notify the Privacy Officer immediately upon receipt of any privacy-related complaint against the Department received by the C/D/O. Provide a copy of all materials received by the C/D/O in connection with the complaint to the Privacy Officer.

c. Cooperate with the Privacy Office in responding, investigating, resolving, or referring complaints.

d. Mitigate, to the extent practicable, any harmful effect that is a result of a complained of use or disclosure of personal, confidential, or sensitive information (including protected health information) in violation of Department policies and procedures or the requirements of state or federal law.

e. Keep all information regarding complaints against the Department confidential and share only on a need-to-know basis and then only to the minimum extent necessary.

Privacy Officer: The Privacy Officer will ensure the Department and its C/D/Os comply with state and federal laws, and department policy, regarding privacy-related complaints against the Department. The Privacy Officer is specifically responsible for the following:

a. Serving as the Department's designated point of contact for privacy-related complaints as required by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Information Practices Act.

b. Developing and making available to the public information and forms necessary for individuals to file a complaint against the Department.

c. Responding, investigating, resolving, or referring all privacy-related complaints against the Department. Including, when expedient, directing affected C/D/Os in responding, investigating, resolving, or referring privacy-related complaints involving the affected C/D/Os. In such cases, the Privacy Officer will provide technical legal assistance to the C/D/Os regarding privacy complaints.

d. Creating and maintaining a Department Privacy Complaint Log which would list each privacy-related complaint against the Department, received by the Department, along with details regarding the response, investigation, resolution, or referral.

e. Retaining all complaint-related materials required to be maintained by, and for the periods of time specified by, applicable state and federal laws and policies.

f. Serving as the Department's point-of-contact/liaison with the Office of Information Security and Privacy Protection, the California Health and Human Services Agency, and all other state and federal agencies, with respect to privacy-related complaints against the Department.

g. Maintaining the Department’s policies and procedures for receiving, responding to, investigating, resolving, referring, and documenting

privacy-related complaints against the Department.

3. References

a. Privacy Office CDPH 6242, Privacy/HIPAA Complaint Form

b. Health Insurance Portability and Accountability Act of 1996 (HIPAA) (45 CFR section 164.530(d))

Policies and Procedures for the Protection of Personal, Confidential and Sensitive Information (Including Protected Health Information) 11-4060

Overview of Department Privacy-Related Policies and Procedures

Pursuant to state law, "[e]ach agency shall establish rules of conduct for persons involved in the design, development, operation, disclosure, or maintenance of records containing personal information . . . ." [Civil Code section 1798.20.] And pursuant to federal law (HIPAA), "[a] covered entity must implement policies and procedures with respect to protected health information that are designed to comply with the standards, implementation specifications, or other requirements of [the Privacy Rule].[45 CFR section 164.530(i)(1).]

The Department's privacy-related policies and procedures consist of and are set forth in:

- This PHAM Chapter 11-Legal, Section 11-4000 "Information Privacy Program", including the Statement of Privacy Policy pursuant to Government Code, Section 11019.9 set forth above in Section 11-4030.

- PHAM Chapter 9. Information Technology Section 9-1000, Information Privacy and Security Policy.

- Department C/D/O-specific policies and procedures maintained by the Department's C/D/Os and administrative units.

Reporting and Responding to Incidents of Unauthorized Access, Use, Disclosure of Personal, Confidential, or Sensitive Information 11-4070

Incident Management and Breach Response Requirements: Both state and federal law require the Department to manage and respond to incidents of possible breaches, and actual breaches, of personal, confidential, and sensitive information (including protected health information). The Department's specific information security and privacy breach requirements and procedures are set forth or referenced in PHAM Chapter 9, Information Technology Section 9-1070, Incident Reporting and Notification.

Roles and Responsibilities: All employees, including contractors, state data custodians,

and volunteer service workers, will understand and discharge their specific responsibilities for implementing and complying with the Department's information security and privacy breach requirements and procedures set forth in PHAM Chapter 9, Information Technology, Section 9-1070, Incident Reporting and Notification.

Notification to Individuals of a Breach of Their Personal Information:

Notice-Triggering Information: State law (Civil Code section 1798.29- Any agency that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California (1) whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person, or, (2) whose encrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the encryption key or security credential was, or is reasonably believed to have been, acquired by an unauthorized person and the agency that owns or licenses the encrypted information has a reasonable belief that the encryption key or security credential could render that personal information readable or usable.

(1) “Personal information” means either of the following:
(A) An individual's first name or first initial and the individual's last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted:
(i) Social security number.
(ii) Driver's license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual.
(iii) Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.
(iv) Medical information.
(v) Health insurance information.
(vi) Unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual. Unique biometric data does not include a physical or digital photograph, unless used or stored for facial recognition purposes.
(vii) Genetic data.
(B) A username or email address in combination with a password or security question and answer that would permit access to an online account.
(2) “Medical information” means any individually identifiable information, in electronic or physical form, regarding the individual's medical history or medical treatment or diagnosis by a health care professional.
(3) “Health insurance information” means an individual's insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's

application and claims history, including any appeals records.

(4) For purposes of this section, “encrypted” means rendered unusable, unreadable, or indecipherable to an unauthorized person through a security technology or methodology generally accepted in the field of information security.

(5) “Genetic data” means any data, regardless of its format, that results from the analysis of a biological sample of an individual, or from another source enabling equivalent information to be obtained and concerns genetic material. Genetic material includes, but is not limited to, deoxyribonucleic acids (DNA), ribonucleic acids (RNA), genes, chromosomes, alleles, genomes, alterations or modifications to DNA or RNA, single nucleotide polymorphisms (SNPs), uninterpreted data that results from analysis of the biological sample or other source, and any information extrapolated, derived, or inferred therefrom.

While Civil Code section 1798.29 focuses on computerized data elements, the current state policy requires notification when a breach of an individual's personal information involves these same "notice-triggering" data elements or otherwise exposes individuals to substantial risk of harm, regardless of the data medium (e.g., paper, oral, etc.). (SAM section 53500).

(Applicable to CDPH HIPAA-Covered Programs Only): Federal law The HIPAA Breach Notification Rule, 45 CFR sections 164.400-414, requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information.

Definition of Breach Under HIPAA:
A breach is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information. An impermissible use or disclosure of protected health information is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on certain risk factors. Managers of the Department's HIPAA-covered healthcare component C/D/Os should consult with the Privacy Officer in determining whether the breach notification requirements apply after a breach involving their C/D/Os information.

2. Roles and Responsibilities (applicable to incidents under HIPAA or IPA)

Center/Division/Office (C/D/O) Managers: C/D/O managers will ensure their C/D/Os comply with the following with respect to breach notifications to individuals:

a. Cooperate with the Privacy Office in determining whether or not notification to individuals is required after a breach. C/D/O managers will provide any additional information requested by the Privacy Officer during its investigation and immediately provide the Privacy Officer with all applicable contracts/agreements if the breach involves a department contractor.

b. In cases where notification to individuals has been determined to be required,

ensure that notification by the program occurs as directed by the Privacy Office.

c. Form, Content, and Timing of Notifications. C/D/Os shall comply with the direction of the Privacy Officer concerning the form, content, and timing of release of all breach notifications issued by the Department.

d. Creating a Breach Notification Log concerning each breach, in a format prescribed by the Privacy Officer, and providing the log to the Privacy Officer.

Privacy Officer: The Privacy Officer will ensure the Department and its C/D/Os comply with state and federal laws, and department policy, regarding breach notification to individuals. The Privacy Officer is specifically responsible for the following:

a. Determining whether or not notification is required in relation to each breach of information security.

b. Providing technical legal assistance to C/D/Os in drafting notifications, responses to notification-related inquiries.

c. Approving all notifications to individuals, prior to release of the notifications.

d. Creating and maintaining a Breach Notification Log concerning each breach that requires notification to individuals.

e. Serving as the Department's point-of-contact/liaison with the Office of Information Security, the California Health and Human Services Agency (CalHHS/Agency), and all other state and federal agencies, with respect to the Department's notifications to individuals.

f. Retaining all breach notification-related materials required to be maintained by, and for the periods of lime specified by, applicable state and federal laws and policies.

g. Maintaining the Department's policies and procedures regarding breach notification by the Department.

3. References

a. California Civil Code section 1798.29.

b. Statewide Information Management Manual (SIMM) section 5340-A) “Incident Reporting and Response Instructions:” and SIMM 5340-C “Requirements to Respond to Incidents Involving a Breach of Personal Information."

c. HIPAA Breach Notification Rule, 45 CFR sections 164.400-414.

Administrative, Technical, and Physical Safeguards to Ensure the Security and Privacy of Personal, Confidential, and Sensitive Information 11-4080

Pursuant to state law, "[e]ach agency shall establish appropriate and reasonable administrative, technical, and physical safeguards to ensure compliance with the provisions of [the IPA], to ensure the security and confidentiality of records, and to protect against anticipated threats or hazards to their security or integrity which could result in any injury." [Civil Code section 1798.21.) And pursuant to federal law (HIPAA), "[a) covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." [45 CFR section 164.530(c)(1).)

The Department's specific administrative, technical, and physical safeguards to ensure the security and privacy of personal, confidential and sensitive Information, including protected health information, are set forth or referenced in PHAM Chapter 9, Information Technology, Section 9-1070. Incident Reporting and Notification.

Roles and Responsibilities: All employees, including contractors, state data custodians, and volunteer service workers, will understand and discharge their specific responsibilities for implementing and complying with the administrative, technical, and physical safeguards set forth in PHAM Chapter 9. Information Technology, Section 9-1070 Incident Reporting and Notification.

Privacy Training 11-4090

State law requires, "Ongoing training and instruction to any persons involved in the design, development, operation, use, disclosure, maintenance, and destruction of records containing personal information about the rules and consequences of noncompliance. (SAM section 5320 and Civil Code section 1798.20)

Federal law (HIPAA) also provide that a HIPAA-covered entity must train all members of its workforce on the policies and procedures with respect to protected health information required by the HIPAA Privacy Rule, as necessary and appropriate for the members of the workforce to carry out their function within the covered entity. [45 CFR section 164.530(b)(1)).]

1. Roles and Responsibilities

    a. The Department's Information Security Office (ISO) and Privacy Office will develop and provide mandatory annual information privacy and security training for all staff.

    b. Before permitting access to department information and information systems, all employees (including managers and contracted staff) must be trained about their privacy and security responsibilities. Supervisors must also be trained about their role and responsibilities for providing day-to-day instruction, training

and supervision of staff regarding their obligation to safeguard personal information.

c. Thereafter, employees must be trained at least once annually to ensure employees continue to understand their responsibilities.

d. Additional or advanced training should also be provided commensurate with increased responsibilities or changes in duties.

e. Both initial and refresher training must cover acceptable rules of behavior and the consequences when rules are not followed.

f. Training must include the rules of telecommuting or telework, and other authorized department remote access programs.

2. References

a. California Civil Code section 1798.20.

b. SAM sections 5320, 5320.1, 5320.2.

c. Health Insurance Portability and Accountability Act of 1996 (HIPAA) 45 CFR section 164.530(b)(1)

Agreements Required for Disclosure of Personal, Confidential, and Sensitive Information to Non-department Persons or Entities 11-4100

1. Written Agreements with Third Parties Required for All Disclosures of Personal Information. The Department is required by state law and policy to ensure that when personal information is shared with third parties, it is either specifically permitted or required by law and that a written agreement is executed between the parties. The written agreement is to identify the applicable federal and state laws, as well as all departmental policies, standards, procedures, and security controls that must be implemented and followed by the third party to adequately protect the information. The agreement must also require the third party, and any of its subcontractors with whom they are authorized to share the data, to share only the minimum personal information necessary, to securely return or destroy the personal information upon expiration of the contract, and to provide immediate notification to the state agency, and to individuals when appropriate, whenever there is a breach of personal information. (SAM section 5305-8, and Civil Code section 1798.19). Department agreements with state and nonstate entities must cover, at a minimum, the following:

c. Appropriate levels of confidentiality for the data based on data classification.
d. Standards for transmission and storage of the data, if applicable.
e. Agreements to comply with all state policy and Law regarding use of information resources and data.
f. Signed confidentiality statements.

g. Agreements to apply security patches and upgrades and keep virus software up to date on all systems on which data may be used.
h. Agreements to notify the Department promptly if a security incident involving the data occurs.

2. Contracting with HIPAA Business Associates (Applicable to CDPH HIPAA-Covered Programs Only).

   HIPAA Business Associate Addendum/Exhibit Applicability: C/D/O staff in one of the Department's covered programs must contact the Privacy Office for guidance in determining if HIPAA requirements apply to a situation and which privacy and security exhibits should be used in an agreement or bid document.

Research Using Vital Records or Program Data **11-4110**

Center/Division/Office (C/D/O) often receive requests from academic and programmatic researchers to use vital records social, demographic, and medical data, or program related data about individuals held in Department data bases. Such disclosures are specifically limited by California law as discussed below. The knowledge generated by these researchers can be of great value for informing the public and government about the impact of policies, programs, and treatment interventions. However, personal information about Californians, regardless of media type (such as electronic, paper, or verbal), must be guarded and protected from misuse, loss, and theft.

The Information Practices Act (IPA) requires all releases of personal information for scientific research be reviewed and approved by the Committee for the Protection of Human Subjects (CPHS) of the California Health and Human Services Agency (CalHHS/Agency). Pursuant to IPA (Civil Code section 1798.24(t)), the CPHS is the Institutional Review Board (IRB) of the CalHHS.

Subdivision (t) of Civil Code Section 1798.24, Health and Safety Code (HSC) Sections 102230, 102231, and 102430 all mandate a detailed protocol be followed before program may release any personal information for scientific research. Due to the specificity and intricacy of these laws and in order to avoid misunderstanding or confusion, contact the appropriate staff listed below.

State agencies releasing identifiable data for research are still required to determine that such releases are permitted by other state and federal legal requirements. CPHS may require letters from programs stating this. See the CPHS link below under Additional Resources. Applicable to CDPH HIPAA-Covered C/D/Os Only: In addition, C/D/Os that are designated by the Department as covered healthcare components of the Department under the Health Insurance Portability and Accountability Act (HIPAA), section 11-4040, above must also comply with HIPAA standards and requirements. HIPAA standards and requirements for handling Personal Health Information (PHI) for research purposes are discussed below.

Requesting Vital Records Data

To request vital records data, visit the Center for Health Statistics and Informatics (CHSI)'s webpage at VSB Data for instructions and applications, and information regarding the new electronic vital statistics data application. In addition, visit the VSB Data Types and Limitations webpage for information about the data products, limitations, and to sign up to the vital records data distribution list to receive notifications of new data products availability.

Data files are subject to cost recovery pursuant to the HSC section 102230.

C/D/Os can request vital records data by submitting an application for surveillance or program evaluation found at the VSB Data Application link above. Additionally, on the same webpage, the C/D/O can request Health Care Access and Information (HCAI) data (formerly OSHPD).

For all additional information related to vital records data requests, contact the Vital Statistics Branch (VSB)'s, Health Information and Research Section (HIRS).

Additional Resources:

- Vital Statistics Advisory Committee (VSAC) information can be found at VSB Vital Statistics Advisory Committee Meeting Information

- Committee for the Protection of Human Subjects (CPHS) application submission information can be found at Committee for the Protection of Human Subjects - HCAI.

- California Cancer Registry (CCR) Data - Researchers may apply to receive death record data linked to the CCR data. For information related to the CCR, contact CCR staff via email or, by mail at California Cancer Registry, 1631 Alhambra Blvd, Suite 200, Sacramento, CA 95816, or by phone at (916) 731-2500.
- Genetic Disease Screening Program (GDSP) Data - Researchers may apply to receive vital records data linked to the California BioBank Program (CBP) patient cohort and maintained within specified CBP variables. For information related to Newborn and Prenatal Screening, contact the CBP via email or by phone at (510) 412-1500. For information related to Birth Defects Monitoring, contact the California Birth Defects Monitoring Program (CBDMP) CBDMP via email or by phone at (916) 341-6404.

- See CalHHS for Information on data from other CalHHS departments.

- Data Request Procedures from other departments will be added as they become available on a website.

Roles and Responsibilities: Before releasing personal information in any format or medium, C/D/O managers will ensure that C/D/O staff is knowledgeable about, and in compliance with appropriate requirements of the:

- IPA requires approval from the Committee for the Protection of Human Subjects (CPHS).
- SAM sections 5300 through 5365.3, including the requirement for data use agreements in section 5310
- Health and Safety Code sections 102230, 102231, and 102430 regarding release of vital records data. Applicable to CDPH HIPAA-Covered C/D/Os Only: In addition, C/D/O managers will also ensure that C/D/O staff is knowledgeable about and in compliance with requirements of HIPAA for handling PHI for research purposes.

References

- California Civil Code section 1798.24(t)
- SAM sections 5300 through 5365.3
- 45 CFR section 164.512(i)

Required Privacy Notices **11-4120**

Notice Required on All CDPH Forms Used to Collect Personal Information: All C/D/Os shall provide on or with any form used to collect personal information from individuals the notice specified in Civil Code section 1798.17. The notice shall include all of the following:

(a) The name of the agency and the division within the agency that is requesting the information.
(b) The title, business address, and telephone number of the agency official who is responsible for the system of records and who shall, upon request, inform an individual regarding the location of his or her records and the categories of any persons who use the information in those records.
(c) The authority, whether granted by statute, regulation, or executive order which authorizes the maintenance of the information.
(d) With respect to each item of information, whether submission of such information is mandatory or voluntary.
(e) The consequences, if any, of not providing all or any part of the requested information.
(f) The principal purpose or purposes within the agency for which the information is to be used.
(g) Any known or foreseeable disclosures which may be made of the information pursuant to subdivision (e) or (f) of Section 1798.24.
(h) The individual's right of access to records containing personal information which are maintained by the agency.

References

- California Civil Code section 1798.17, “Notice; [periodic provision; contents.”
- SAM section 5310.1, “State entity Privacy Statement and Notice on Collection.”
- 45 CFR section 164.520, “Notice of Privacy Practices for Protected Health Information.”

Privacy Threshold Assessments (PTA) and Privacy Impact Assessments (PIA)

Introduction 11-4130

State and federal policy and regulation require a C/D/O to conduct Privacy Impact Assessments (PIAs) on information systems that collect, create, maintain, distribute, or dispose of personal information, as defined in California Civil Code section 1798.3. The PIA is required to identify privacy and security risks and protections throughout the life cycle of personal information collected to support business processes. PIAs are also conducted to ensure information systems that contain or use personal information comply with legal, regulatory, and policy requirements regarding privacy and information security. The PIA documents the privacy and information security risks and controls in place to protect the personal information being collected, used, maintained, stored, and disposed of within the Department.

The Department uses Privacy Threshold Assessments (PTAs) to determine which C/D/O information systems contain or use personal information and require PIAs. A PTA is completed by the C/D/O for each information system and submitted to the CDPH Privacy Office. Along with the Information Security Office, the Privacy Office will determine if a PIA is required.

General information about the PTA and PIA can be found on the Privacy Office webpage. Questions or guidance about completing a PTA or PIA should be directed to the Information Security Office (ISO) or Privacy Office.

References

a. California Civil Code section 1798.21
b. California Government Code section 11549.3
c. SAM section 5310.8
d. SIMM section 5310-C
e. NIST SP 800-53 revision 5

Definitions 11-4140

“Business Process Owners” include C/D/O managers and workforce members responsible for information access and use.

“Data Custodians” include Information Technology managers and workforce members responsible as caretaker for the proper use and protection of information assets on behalf of the information asset owner.

“Information System” includes databases of organized information containing one or more records, which are maintained by CDPH, from which information is retrievable by the name of an individual or by a unique identifier.

“Material Change” includes but is not limited to the maintenance of additional data elements, sharing of information with additional entities, and significant adjustments to a system’s security controls.

"C/D/O Managers" include information asset owner deputy directors and managers having responsibility for making classification, categorization, and control decisions regarding information assets.

Privacy Threshold Assessments 11-4150

Each C/D/O shall conduct a PTA for all new Information Systems, upon selection of system architecture, and any existing Information System that undergoes a Material Change. The Privacy Office shall provide the link to the PTA to each program when a PTA is indicated. A C/D/O may also request the link if it believes the PTA is necessary by emailing Privacy Assessments.

Each C/D/O shall complete the PTA within fourteen (14) calendar days of receiving notification that a PTA is required from the Privacy Office and the link to the PTA form.

The PTA completed by the information asset owner will be evaluated by the Department's Privacy Office and Information Security Office.

References

a. California Civil Code section 1798.21
b. California Government Code section 11549.3
c. SAM section 5310.8
d. SIMM section 5310-C
e. NIST SP 800-53 revision 5

Privacy Impact Assessments 11-4160

If the PTA identifies that an Information System collects, creates, maintains, uses, or sends sensitive or confidential information, including personal information, the Privacy Office will notify the C/D/O that it must complete a PIA. The Privacy Office shall provide the PIA to each C/D/O when a PIA is indicated.

A PIA shall be conducted by the C/D/O when indicated by a PTA for all new Information Systems, upon selection of system architecture or, or for existing Information Systems that undergo a Material Change.

The PIA is completed by the business unit responsible for making decisions regarding the information asset (information asset owner) with assistance from knowledgeable C/D/O personnel and Information Technology (IT) systems owners/data custodians.

The C/D/O must return the completed PIA to the Privacy Office at within thirty (30) calendar days of receiving notification from the Privacy Office that a PIA is required.

The Departments Privacy Office, in conjunction with the Information Security Office, shall review each PIA and recommend any necessary mitigation and/or corrective actions to the C/D/O that owns the Information System being evaluated. The C/D/O that owns the Information System shall incorporate the recommendations from the Privacy Office and the Information Security Office to the Information System.

References

a. California Civil Code section 1798.21
b. California Government Code section 11549.3
c. SAM section 5310.8
d. SIMM section 5310-C
e. NIST SP 800-53 revision 5

Roles And Responsibilities **11-4170**

Privacy Office:

The Departments Privacy Officer, or designee, is responsible for:

- Overseeing the Department's implementation of PTA and PIA policy and compliance with State and Federal privacy laws, including the California Information Practices Act (IPA) and the Federal Health Insurance Portability and Accountability Act (HIPAA) privacy regulations.

- Training the Departments workforce members on PTA and PIA policy and legal requirements.

- Assisting C/D/O management with completing a PTA, and if appropriate, a PIA, on all existing Information Systems, all new Information Systems and any existing Information System that undergoes a Material Change.

- Reviewing all PIAs conducted for Information Systems.

- Tracking and monitoring of completed PTAs and PIAs.

- Supporting periodic auditing and assessment of compliance with the policy.

- Managing the policy throughout its lifecycle from development to decommissioning or archiving and communicating key notifications regarding the policy such as decommissioning to linked policies, procedures, standards, and guidelines to relevant stakeholders.

- Participating in the security and privacy policy variance process and assessing the risks and compliance plan associated with variance requests.

- Including the requirements for PTAs and PIAs in executed contracts with contractors/sub-contractors, when necessary.

Information Security Office/Information Technology Services Division:

The Department's Information Security Officer, or designee, is responsible for:

- Assisting the Privacy Office to ensure that all existing Information Systems, all new Information Systems and any existing Information System that undergoes a Material Change conduct a PTA and if appropriate, a PIA.

- Reviewing all PIAs and PTAs conducted for the Department's Information Systems.

The Department's Chief Information Officer, or designee, is responsible for:

- Ensuring PTAs, and PIAs when indicated, are completed during the Project Approval Lifecycle.

Business Process Owners, Data Custodians and/or C/D/O Management

Business Process Owners, Data Custodians, and C/D/O Managers, or their designees, are responsible for:

- Assisting the Privacy Office in maintaining accountings of disclosures as required by State and Federal privacy laws, including the IPA and HIPAA.

- Assisting the Privacy Office by completing all requested PTAs and PIAs within the required timeframes.

Users

The Department Users are responsible for:

- Familiarizing themselves with PTA and PIA policies and associated procedures.

- Reporting incidents of possible misuse or violation of this policy to the Privacy Officer, Information Security Officer, designee or appropriate security/privacy staff.

- Reading and adhering to this policy and applicable the Department's information security and privacy policies.

References

a. California Civil Code section 1798.21
b. California Government Code section 11549.3
c. SAM section 5310.8
d. SIMM section 5310-C
e. NIST SP 800-53 revision 5