



Table of Contents	
State Law On Breach	2
Medical Records Release Laws Including Minors and Mental Health Records Release	10
Identity Theft	23
Communicable Diseases and HIV/AIDS Reporting	26
Medical Record Copying Fees	34
References and Resources	35

Total Medical Compliance has created state-specific guidelines as a resource for our clients. This information is not intended as legal advice and may not cover all areas of compliance. TMC encourages clients to research and consult with your state agencies to remain up-to-date on any changes.

STATE LAW ON BREACH**Assembly Bill No. 2828**

An act to amend Sections 1798.29 and 1798.82 of the Civil Code, relating to personal information.
 [Approved by Governor September 13, 2016. Filed with Secretary of State September 13, 2016.]

SECTION 1. Section 1798.29 of the Civil Code is amended to read:

1798.29. (a) 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 useable. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(b) Any agency that maintains computerized data that includes personal information that the agency does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.

(d) Any agency that is required to issue a security breach notification pursuant to this section shall meet all of the following requirements:

(1) The security breach notification shall be written in plain language, shall be titled "Notice of Data Breach," and shall present the information described in paragraph (2) under the following headings: "What Happened," "What Information Was Involved," "What We Are Doing," "What You Can Do," and "For More Information." Additional information may be provided as a supplement to the notice.

(A) The format of the notice shall be designed to call attention to the nature and significance of the information it contains.

(B) The title and headings in the notice shall be clearly and conspicuously displayed.

(C) The text of the notice and any other notice provided pursuant to this section shall be no smaller than 10-point type.

(D) For a written notice described in paragraph (1) of subdivision (i), use of the model security breach notification form prescribed below or use of the headings described in this paragraph with the information described in paragraph (2), written in plain language, shall be deemed to be in compliance with this subdivision.

[NAME OF INSTITUTION / LOGO] ____ Date: [insert date]

NOTICE OF DATA BREACH

What Happened?

What Information Was Involved?

What We Are Doing.

What You Can Do.

Other Important Information.
[insert other important information]

(E) For an electronic notice described in paragraph (2) of subdivision (i), use of the headings described in this paragraph with the information described in paragraph (2), written in plain language, shall be deemed to be in compliance with this subdivision.

(2) The security breach notification described in paragraph (1) shall include, at a minimum, the following information: (A) The name and contact information of the reporting agency subject to this section. (B) A list of the types of personal information that were or are reasonably believed to have been the subject of a breach. (C) If the information is possible to determine at the time the notice is provided, then any of the following: (i) the date of the breach, (ii) the estimated date of the breach, or (iii) the date range within which the breach occurred. The notification shall also include the date of the notice. (D) Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided. (E) A general description of the breach incident, if that information is possible to determine at the time the notice is provided. (F) The toll-free telephone numbers and addresses of the major credit reporting agencies, if the breach exposed a social security number or a driver's license or California identification card number. (3) At the discretion of the agency, the security breach notification may also include any of the following: (A) Information about what the agency has done to protect individuals whose information has been breached. (B) Advice on steps that the person whose information has been breached may take to protect himself or herself.

(e) Any agency that is required to issue a security breach notification pursuant to this section to more than 500 California residents as a result of a single breach of the security system shall electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the Attorney General. A single sample copy of a security breach notification shall not be deemed to be within subdivision (f) of Section 6254 of the Government Code.

(f) For purposes of this section, "breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the agency. Good faith acquisition of personal information by an employee or agent of the agency for the purposes of the agency is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

(g) For purposes of this section, "personal information" means either of the following: (1) An individual's first name or first initial and 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: (A) Social security number. (B) Driver's license number or California identification card number. (C) 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. (D) Medical information. (E) Health insurance information. (F) Information or data collected through the use or operation of an automated license plate recognition system, as defined in Section 1798.90.5. (2) A user name or email address, in combination with a password or security question and answer that would permit access to an online account.

(h) (1) For purposes of this section, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records. (2) For purposes of this section, "medical information" means any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional. (3) For purposes of this section, "health insurance information" means an individual's health 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.

(i) For purposes of this section, "notice" may be provided by one of the following methods:

(1) Written notice.(2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code.(3) Substitute notice, if the agency demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars (\$250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the agency does not have sufficient contact information.

Substitute notice shall consist of all of the following:(A) Email notice when the agency has an email address for the subject persons.(B) Conspicuous posting, for a minimum of 30 days, of the notice on the agency's Internet Web site page, if the agency maintains one. For purposes of this subparagraph, conspicuous posting on the agency's Internet Web site means providing a link to the notice on the home page or first significant page after entering the Internet Web site that is in larger type than the surrounding text, or in contrasting type, font, or color to the surrounding text of the same size, or set off from the surrounding text of the same size by symbols or other marks that call attention to the link.(C) Notification to major statewide media and the Office of Information Security within the Department of Technology.(4) In the case of a breach of the security of the system involving personal information defined in paragraph (2) of subdivision (g) for an online account, and no other personal information defined in paragraph (1) of subdivision (g), the agency may comply with this section by providing the security breach notification in electronic or other form that directs the person whose personal information has been breached to promptly change his or her password and security question or answer, as applicable, or to take other steps appropriate to protect the online account with the agency and all other online accounts for which the person uses the same user name or email address and password or security question or answer.

(5) In the case of a breach of the security of the system involving personal information defined in paragraph (2) of subdivision (g) for login credentials of an email account furnished by the agency, the agency shall not comply with this section by providing the security breach notification to that email address, but may, instead, comply with this section by providing notice by another method described in this subdivision or by clear and conspicuous notice delivered to the resident online when the resident is connected to the online account from an Internet Protocol address or online location from which the agency knows the resident customarily accesses the account.

(j) Notwithstanding subdivision (i), an agency that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this part shall be deemed to be in compliance with the notification requirements of this section if it notifies subject persons in accordance with its policies in the event of a breach of security of the system.

(k) Notwithstanding the exception specified in paragraph (4) of subdivision (b) of Section 1798.3, for purposes of this section, "agency" includes a local agency, as defined in subdivision (a) of Section 6252 of the Government Code.

(l) For purposes of this section, "encryption key" and "security credential" mean the confidential key or process designed to render the data useable, readable, and decipherable.

SEC. 2. Section 1798.82 of the Civil Code is amended to read:

1798.82. (a) A person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a 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 person or business 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 useable. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(b) A person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of the breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made promptly after the law enforcement agency determines that it will not compromise the investigation.

(d) A person or business that is required to issue a security breach notification pursuant to this section shall meet all of the following requirements: (1) The security breach notification shall be written in plain language, shall be titled "Notice of Data Breach," and shall present the information described in paragraph (2) under the following headings: "What Happened," "What Information Was Involved," "What We Are Doing," "What You Can Do," and "For More Information." Additional information may be provided as a supplement to the notice. (A) The format of the notice shall be designed to call attention to the nature and significance of the information it contains. (B) The title and headings in the notice shall be clearly and conspicuously displayed. (C) The text of the notice and any other notice provided pursuant to this section shall be no smaller than 10-point type. (D) For a written notice described in paragraph (1) of subdivision (j), use of the model security breach notification form prescribed below or use of the headings described in this paragraph with the information described in paragraph (2), written in plain language, shall be deemed to be in compliance with this subdivision.

[NAME OF INSTITUTION / LOGO] ____ ____ Date: [insert date]

NOTICE OF DATA BREACH

What Happened?

What Information Was Involved?

What We Are Doing.

What You Can Do.

Other Important Information.
[insert other important information]

(E) For an electronic notice described in paragraph (2) of subdivision (j), use of the headings described in this paragraph with the information described in paragraph (2), written in plain language, shall be deemed to be in compliance with this subdivision.

(2) The security breach notification described in paragraph (1) shall include, at a minimum, the following information: (A) The name and contact information of the reporting person or business subject to this section. (B) A list of the types of personal information that were or are reasonably believed to have been the subject of a breach. (C) If the information is possible to determine at the time the notice is provided, then any of the following: (i) the date of the breach, (ii) the estimated date of the breach, or (iii) the date range within which the breach occurred. The notification shall also include the date of the notice. (D) Whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided. (E) A general description of the breach incident, if that information is possible to determine at the time the notice is provided. (F) The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a social security number or a driver's license or California identification card number. (G) If the person or business providing the notification was the source of the breach, an offer to provide appropriate identity theft prevention and mitigation services, if any, shall be provided at no cost to the affected person for not less than 12 months along with all information necessary to take advantage of the offer to any person whose information was or may have been breached if the breach exposed or may have exposed personal information defined in subparagraphs (A) and (B) of paragraph (1) of subdivision (h). (3) At the discretion of the person or business, the security breach notification may also include any of the following: (A) Information about what the person or business has done to protect individuals whose information has been breached. (B) Advice on steps that the person whose information has been breached may take to protect himself or herself.

(e) A covered entity under the federal Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. Sec. 1320d et seq.) will be deemed to have complied with the notice requirements in subdivision (d) if it has complied completely with Section 13402(f) of the federal Health Information Technology for Economic and Clinical Health Act (Public Law 111-5). However, nothing in this subdivision shall be construed to exempt a covered entity from any other provision of this section.

(f) A person or business that is required to issue a security breach notification pursuant to this section to more than 500 California residents as a result of a single breach of the security system shall electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the Attorney General. A single sample copy of a security breach notification shall not be deemed to be within subdivision (f) of Section 6254 of the Government Code.

(g) For purposes of this section, "breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

(h) For purposes of this section, "personal information" means either of the following: (1) An individual's first name or first initial and 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: (A) Social security number. (B) Driver's license number or California identification card number. (C) 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.(D) Medical information.(E) Health insurance information.(F) Information or data collected through the use or operation of an automated license plate recognition system, as defined in Section 1798.90.5.(2) A user name or email address, in combination with a password or security question and answer that would permit access to an online account.

(i) (1) For purposes of this section, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.(2) For purposes of this section, "medical information" means any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional.(3) For purposes of this section, "health insurance information" means an individual's health 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.

(j) For purposes of this section, "notice" may be provided by one of the following methods:(1) Written notice.(2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code.(3) Substitute notice, if the person or business demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars (\$250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the person or business does not have sufficient contact information. Substitute notice shall consist of all of the following:(A) Email notice when the person or business has an email address for the subject persons.(B) Conspicuous posting, for a minimum of 30 days, of the notice on the Internet Web site page of the person or business, if the person or business maintains one. For purposes of this subparagraph, conspicuous posting on the person's or business's Internet Web site means providing a link to the notice on the home page or first significant page after entering the Internet Web site that is in larger type than the surrounding text, or in contrasting type, font, or color to the surrounding text of the same size, or set off from the surrounding text of the same size by symbols or other marks that call attention to the link.(C) Notification to major statewide media.(4) In the case of a breach of the security of the system involving personal information defined in paragraph (2) of subdivision (h) for an online account, and no other personal information defined in paragraph (1) of subdivision (h), the person or business may comply with this section by providing the security breach notification in electronic or other form that directs the person whose personal information has been breached promptly to change his or her password and security question or answer, as applicable, or to take other steps appropriate to protect the online account with the person or business and all other online accounts for which the person whose personal information has been breached uses the same user name or email address and password or security question or answer.(5) In the case of a breach of the security of the system involving personal information defined in paragraph (2) of subdivision (h) for login credentials of an email account furnished by the person or business, the person or business shall not comply with this section by providing the security breach notification to that email address, but may, instead, comply with this section by providing notice by another method described in this subdivision or by clear and conspicuous notice delivered to the resident online when the resident is connected to the online account from an Internet Protocol address or online

location from which the person or business knows the resident customarily accesses the account.
 (k) For purposes of this section, "encryption key" and "security credential" mean the confidential key or process designed to render data useable, readable, and decipherable.

(l) Notwithstanding subdivision (j), a person or business that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this part, shall be deemed to be in compliance with the notification requirements of this section if the person or business notifies subject persons in accordance with its policies in the event of a breach of security of the system.

MEDICAL RECORDS RELEASE LAWS (Including minor and mental health records)

CONFIDENTIALITY OF MEDICAL INFORMATION ACT CALIFORNIA CIVIL CODE SECTIONS 56-56.16

56.05. For purposes of this part:

(a) "Authorization" means permission granted in accordance with Section 56.11 or 56.21 for the disclosure of medical information.

(b) "Authorized recipient" means any person who is authorized to receive medical information pursuant to Section 56.10 or 56.20.

(c) "Confidential communications request" means a request by a subscriber or enrollee that health care service plan communications containing medical information be communicated to him or her at a specific mail or email address or specific telephone number, as designated by the subscriber or enrollee.

(d) "Contractor" means any person or entity that is a medical group, independent practice association, pharmaceutical benefits manager, or a medical service organization and is not a health care service plan or provider of health care. "Contractor" does not include insurance institutions as defined in subdivision (k) of Section 791.02 of the Insurance Code or pharmaceutical benefits managers licensed pursuant to the Knox-Keene Health Care Service Plan Act of 1975 (Chapter 2.2 (commencing with Section 1340) of Division 2 of the Health and Safety Code).

(e) "Endanger" means that the subscriber or enrollee fears that disclosure of his or her medical information could subject the subscriber or enrollee to harassment or abuse.

(f) "Enrollee" has the same meaning as that term is defined in Section 1345 of the Health and Safety Code.

(g) "Health care service plan" means any entity regulated pursuant to the Knox-Keene Health Care Service Plan Act of 1975 (Chapter 2.2 (commencing with Section 1340) of Division 2 of the Health and Safety Code).

(h) "Licensed health care professional" means any person licensed or certified pursuant to Division 2 (commencing with Section 500) of the Business and Professions Code, the Osteopathic Initiative Act or the Chiropractic Initiative Act, or Division 2.5 (commencing with Section 1797) of the Health and Safety Code.

(i) "Marketing" means to make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service. "Marketing" does not include any of the following: (1) Communications made orally or in writing for which the communicator does not receive direct or indirect remuneration, including, but not limited to, gifts, fees, payments, subsidies, or other economic benefits, from a third party for making the

communication. (2) Communications made to current enrollees solely for the purpose of describing a provider's participation in an existing health care provider network or health plan network of a Knox-Keene licensed health plan to which the enrollees already subscribe; communications made to current enrollees solely for the purpose of describing if, and the extent to which, a product or service, or payment for a product or service, is provided by a provider, contractor, or plan or included in a plan of benefits of a Knox-Keene licensed health plan to which the enrollees already subscribe; or communications made to plan enrollees describing the availability of more cost-effective pharmaceuticals. (3) Communications that are tailored to the circumstances of a particular individual to educate or advise the individual about treatment options, and otherwise maintain the individual's adherence to a prescribed course of medical treatment, as provided in Section 1399.901 of the Health and Safety Code, for a chronic and seriously debilitating or life-threatening condition as defined in subdivisions (d) and (e) of Section 1367.21 of the Health and Safety Code, if the health care provider, contractor, or health plan receives direct or indirect remuneration, including, but not limited to, gifts, fees, payments, subsidies, or other economic benefits, from a third party for making the communication, if all of the following apply: (A) The individual receiving the communication is notified in the communication in typeface no smaller than 14-point type of the fact that the provider, contractor, or health plan has been remunerated and the source of the remuneration. (B) The individual is provided the opportunity to opt out of receiving future remunerated communications. (C) The communication contains instructions in typeface no smaller than 14-point type describing how the individual can opt out of receiving further communications by calling a toll-free number of the health care provider, contractor, or health plan making the remunerated communications. No further communication may be made to an individual who has opted out after 30 calendar days from the date the individual makes the opt out request.

(j) "Medical information" means any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care, health care service plan, pharmaceutical company, or contractor regarding a patient's medical history, mental or physical condition, or treatment. "Individually identifiable" means that the medical information includes or contains any element of personal identifying information sufficient to allow identification of the individual, such as the patient's name, address, electronic mail address, telephone number, or social security number, or other information that, alone or in combination with other publicly available information, reveals the individual's identity.

(k) "Patient" means any natural person, whether or not still living, who received health care services from a provider of health care and to whom medical information pertains.

(l) "Pharmaceutical company" means any company or business, or an agent or representative thereof, that manufactures, sells, or distributes pharmaceuticals, medications, or prescription drugs. "Pharmaceutical company" does not include a pharmaceutical benefits manager, as included in subdivision (c), or a provider of health care.

(m) "Provider of health care" means any person licensed or certified pursuant to Division 2 (commencing with Section 500) of the Business and Professions Code; any person licensed pursuant to the Osteopathic Initiative Act or the Chiropractic Initiative Act; any person certified pursuant to Division 2.5 (commencing with Section 1797) of the Health and Safety Code; any clinic, health dispensary, or health facility licensed pursuant to Division 2 (commencing with Section 1200) of the Health and Safety Code. "Provider of health care" does not include insurance institutions as defined in subdivision (k) of Section 791.02 of the Insurance Code.

(n) "Sensitive services" means all health care services described in Sections 6924, 6925, 6926, 6927, 6928, and 6929 of the Family Code, and Sections 121020 and 124260 of the Health and Safety

Code, obtained by a patient at or above the minimum age specified for consenting to the service specified in the section.

(o) "Subscriber" has the same meaning as that term is defined in Section 1345 of the Health and Safety Code.

56.06. (a) Any business organized for the purpose of maintaining medical information, as defined in subdivision (g) of Section 56.05, in order to make the information available to an individual or to a provider of health care at the request of the individual or a provider of health care, for purposes of allowing the individual to manage his or her information, or for the diagnosis and treatment of the individual, shall be deemed to be a provider of health care subject to the requirements of this part. However, nothing in this section shall be construed to make a business specified in this subdivision a provider of health care for purposes of any law other than this part, including laws that specifically incorporate by reference the definitions of this part.

(b) Any business that offers software or hardware to consumers, including a mobile application or other related device that is designed to maintain medical information, as defined in subdivision (g) of Section 56.05, in order to make the information available to an individual or a provider of health care at the request of the individual or a provider of health care, for purposes of allowing the individual to manage his or her information, or for the diagnosis, treatment, or management of a medical condition of the individual, shall be deemed to be a provider of health care subject to the requirements of this part. However, nothing in this section shall be construed to make a business specified in this subdivision a provider of health care for purposes of any law other than this part, including laws that specifically incorporate by reference the definitions of this part.

(c) Any business described in subdivision (a) or (b) shall maintain the same standards of confidentiality required of a provider of health care with respect to medical information disclosed to the business.

(d) Any business described in subdivision (a) or (b) shall be subject to the penalties for improper use and disclosure of medical information prescribed in this part.

56.07. (a) Except as provided in subdivision (c), upon the patient's written request, any corporation described in Section 56.06, or any other entity that compiles or maintains medical information for any reason, shall provide the patient, at no charge, with a copy of any medical profile, summary, or information maintained by the corporation or entity with respect to the patient. (b) A request by a patient pursuant to this section shall not be deemed to be an authorization by the patient for the release or disclosure of any information to any person or entity other than the patient. (c) This section shall not apply to any patient records that are subject to inspection by the patient pursuant to Section 123110 of the Health and Safety Code and shall not be deemed to limit the right of a health care provider to charge a fee for the preparation of a summary of patient records as provided in Section 123130 of the Health and Safety Code. This section shall not apply to a health care service plan licensed pursuant to Chapter 2.2 (commencing with Section 1340) of Division 2 of the Health and Safety Code or a disability insurer licensed pursuant to the Insurance Code. This section shall not apply to medical information compiled or maintained by a fire and casualty insurer or its retained counsel in the regular course of investigating or litigating a claim under a policy of insurance that it has written. For the purposes of this section, a fire and casualty insurer is an insurer writing policies that may be sold by a fire and casualty licensee pursuant to Section 1625 of the Insurance Code.

56.10. (a) A provider of health care, health care service plan, or contractor shall not disclose medical information regarding a patient of the provider of health care or an enrollee or subscriber of a health care service plan without first obtaining an authorization, except as provided in subdivision (b) or (c).

(b) A provider of health care, a health care service plan, or a contractor shall disclose medical information if the disclosure is compelled by any of the following: (1) By a court pursuant to an order of that court. (2) By a board, commission, or administrative agency for purposes of adjudication pursuant to its lawful authority. (3) By a party to a proceeding before a court or administrative agency pursuant to a subpoena, subpoena duces tecum, notice to appear served pursuant to Section 1987 of the Code of Civil Procedure, or any provision authorizing discovery in a proceeding before a court or administrative agency.

(4) By a board, commission, or administrative agency pursuant to an investigative subpoena issued under Article 2 (commencing with Section 11180) of Chapter 2 of Part 1 of Division 3 of Title 2 of the Government Code. (5) By an arbitrator or arbitration panel, when arbitration is lawfully requested by either party, pursuant to a subpoena duces tecum issued under Section 1282.6 of the Code of Civil Procedure, or another provision authorizing discovery in a proceeding before an arbitrator or arbitration panel. (6) By a search warrant lawfully issued to a governmental law enforcement agency. (7) By the patient or the patient's representative pursuant to Chapter 1 (commencing with Section 123100) of Part 1 of Division 106 of the Health and Safety Code. (8) By a coroner, when requested in the course of an investigation by the coroner's office for the purpose of identifying the decedent or locating next of kin, or when investigating deaths that may involve public health concerns, organ or tissue donation, child abuse, elder abuse, suicides, poisonings, accidents, sudden infant deaths, suspicious deaths, unknown deaths, or criminal deaths, or upon notification of, or investigation of, imminent deaths that may involve organ or tissue donation pursuant to Section 7151.15 of the Health and Safety Code, or when otherwise authorized by the decedent's representative. Medical information requested by the coroner under this paragraph shall be limited to information regarding the patient who is the decedent and who is the subject of the investigation or who is the prospective donor and shall be disclosed to the coroner without delay upon request. (9) When otherwise specifically required by law.

(c) A provider of health care or a health care service plan may disclose medical information as follows: (1) The information may be disclosed to providers of health care, health care service plans, contractors, or other health care professionals or facilities for purposes of diagnosis or treatment of the patient. This includes, in an emergency situation, the communication of patient information by radio transmission or other means between emergency medical personnel at the scene of an emergency, or in an emergency medical transport vehicle, and emergency medical personnel at a health facility licensed pursuant to Chapter 2 (commencing with Section 1250) of Division 2 of the Health and Safety Code. (2) The information may be disclosed to an insurer, employer, health care service plan, hospital service plan, employee benefit plan, governmental authority, contractor, or other person or entity responsible for paying for health care services rendered to the patient, to the extent necessary to allow responsibility for payment to be determined and payment to be made. If (A) the patient is, by reason of a comatose or other disabling medical condition, unable to consent to the disclosure of medical information and (B) no other arrangements have been made to pay for the health care services being rendered to the patient, the information may be disclosed to a governmental authority to the extent necessary to determine the patient's eligibility for, and to obtain, payment under a governmental program for health care services provided to the patient. The information may also be disclosed to another provider of health care or health care service plan

as necessary to assist the other provider or health care service plan in obtaining payment for health care services rendered by that provider of health care or health care service plan to the patient.

(3) The information may be disclosed to a person or entity that provides billing, claims management, medical data processing, or other administrative services for providers of health care or health care service plans or for any of the persons or entities specified in paragraph (2).

However, information so disclosed shall not be further disclosed by the recipient in a way that would violate this part. (4) The information may be disclosed to organized committees and agents of professional societies or of medical staffs of licensed hospitals, licensed health care service plans, professional standards review organizations, independent medical review organizations and their selected reviewers, utilization and quality control peer review organizations as established by Congress in Public Law 97-248 in 1982, contractors, or persons or organizations insuring, responsible for, or defending professional liability that a provider may incur, if the committees, agents, health care service plans, organizations, reviewers, contractors, or persons are engaged in reviewing the competence or qualifications of health care professionals or in reviewing health care services with respect to medical necessity, level of care, quality of care, or justification of charges.

(5) The information in the possession of a provider of health care or health care service plan may be reviewed by a private or public body responsible for licensing or accrediting the provider of health care or health care service plan. However, no patient-identifying medical information may be removed from the premises except as expressly permitted or required elsewhere by law, nor shall that information be further disclosed by the recipient in a way that would violate this part. (6) The information may be disclosed to the county coroner in the course of an investigation by the coroner's office when requested for all purposes not included in paragraph (8) of subdivision (b).

(7) The information may be disclosed to public agencies, clinical investigators, including investigators conducting epidemiologic studies, health care research organizations, and accredited public or private nonprofit educational or health care institutions for bona fide research purposes. However, no information so disclosed shall be further disclosed by the recipient in a way that would disclose the identity of a patient or violate this part. (8) A provider of health care or health care service plan that has created medical information as a result of employment-related health care services to an employee conducted at the specific prior written request and expense of the employer may disclose to the employee's employer that part of the information that: (A) Is relevant in a lawsuit, arbitration, grievance, or other claim or challenge to which the employer and the employee are parties and in which the patient has placed in issue his or her medical history, mental or physical condition, or treatment, provided that information may only be used or disclosed in connection with that proceeding. (B) Describes functional limitations of the patient that may entitle the patient to leave from work for medical reasons or limit the patient's fitness to perform his or her present employment, provided that no statement of medical cause is included in the information disclosed. (9) Unless the provider of health care or a health care service plan is notified in writing of an agreement by the sponsor, insurer, or administrator to the contrary, the information may be disclosed to a sponsor, insurer, or administrator of a group or individual insured or uninsured plan or policy that the patient seeks coverage by or benefits from, if the information was created by the provider of health care or health care service plan as the result of services conducted at the specific prior written request and expense of the sponsor, insurer, or administrator for the purpose of evaluating the application for coverage or benefits. (10) The information may be disclosed to a health care service plan by providers of health care that contract with the health care service plan and may be transferred among providers of health care that contract with the health care service plan, for the purpose of administering the health care service

plan. Medical information shall not otherwise be disclosed by a health care service plan except in accordance with this part. (11) This part does not prevent the disclosure by a provider of health care or a health care service plan to an insurance institution, agent, or support organization, subject to Article 6.6 (commencing with Section 791) of Chapter 1 of Part 2 of Division 1 of the Insurance Code, of medical information if the insurance institution, agent, or support organization has complied with all of the requirements for obtaining the information pursuant to Article 6.6 (commencing with Section 791) of Chapter 1 of Part 2 of Division 1 of the Insurance Code. (12) The information relevant to the patient's condition, care, and treatment provided may be disclosed to a probate court investigator in the course of an investigation required or authorized in a conservatorship proceeding under the Guardianship-Conservatorship Law as defined in Section 1400 of the Probate Code, or to a probate court investigator, probation officer, or domestic relations investigator engaged in determining the need for an initial guardianship or continuation of an existing guardianship. (13) The information may be disclosed to an organ procurement organization or a tissue bank processing the tissue of a decedent for transplantation into the body of another person, but only with respect to the donating decedent, for the purpose of aiding the transplant. For the purpose of this paragraph, "tissue bank" and "tissue" have the same meanings as defined in Section 1635 of the Health and Safety Code. (14) The information may be disclosed when the disclosure is otherwise specifically authorized by law, including, but not limited to, the voluntary reporting, either directly or indirectly, to the federal Food and Drug Administration of adverse events related to drug products or medical device problems, or to disclosures made pursuant to subdivisions (b) and (c) of Section 11167 of the Penal Code by a person making a report pursuant to Sections 11165.9 and 11166 of the Penal Code, provided that those disclosures concern a report made by that person. (15) Basic information, including the patient's name, city of residence, age, sex, and general condition, may be disclosed to a state-recognized or federally recognized disaster relief organization for the purpose of responding to disaster welfare inquiries. (16) The information may be disclosed to a third party for purposes of encoding, encrypting, or otherwise anonymizing data. However, no information so disclosed shall be further disclosed by the recipient in a way that would violate this part, including the unauthorized manipulation of coded or encrypted medical information that reveals individually identifiable medical information. (17) For purposes of disease management programs and services as defined in Section 1399.901 of the Health and Safety Code, information may be disclosed as follows: (A) to an entity contracting with a health care service plan or the health care service plan's contractors to monitor or administer care of enrollees for a covered benefit, if the disease management services and care are authorized by a treating physician, or (B) to a disease management organization, as defined in Section 1399.900 of the Health and Safety Code, that complies fully with the physician authorization requirements of Section 1399.902 of the Health and Safety Code, if the health care service plan or its contractor provides or has provided a description of the disease management services to a treating physician or to the health care service plan's or contractor's network of physicians. This paragraph does not require physician authorization for the care or treatment of the adherents of a well-recognized church or religious denomination who depend solely upon prayer or spiritual means for healing in the practice of the religion of that church or denomination. (18) The information may be disclosed, as permitted by state and federal law or regulation, to a local health department for the purpose of preventing or controlling disease, injury, or disability, including, but not limited to, the reporting of disease, injury, vital events, including, but not limited to, birth or death, and the conduct of public health surveillance, public health investigations, and public health interventions, as authorized or required by state or federal law or regulation. (19) The information may be disclosed, consistent

with applicable law and standards of ethical conduct, by a psychotherapist, as defined in Section 1010 of the Evidence Code, if the psychotherapist, in good faith, believes the disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a reasonably foreseeable victim or victims, and the disclosure is made to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat. (20) The information may be disclosed as described in Section 56.103. (21) (A) The information may be disclosed to an employee welfare benefit plan, as defined under Section 3(1) of the Employee Retirement Income Security Act of 1974 (29 U.S.C. Sec. 1002(1)), which is formed under Section 302(c)(5) of the Taft-Hartley Act (29 U.S.C. Sec. 186(c)(5)), to the extent that the employee welfare benefit plan provides medical care, and may also be disclosed to an entity contracting with the employee welfare benefit plan for billing, claims management, medical data processing, or other administrative services related to the provision of medical care to persons enrolled in the employee welfare benefit plan for health care coverage, if all of the following conditions are met: (i) The disclosure is for the purpose of determining eligibility, coordinating benefits, or allowing the employee welfare benefit plan or the contracting entity to advocate on the behalf of a patient or enrollee with a provider, a health care service plan, or a state or federal regulatory agency. (ii) The request for the information is accompanied by a written authorization for the release of the information submitted in a manner consistent with subdivision (a) and Section 56.11. (iii) The disclosure is authorized by and made in a manner consistent with the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191). (iv) Any information disclosed is not further used or disclosed by the recipient in any way that would directly or indirectly violate this part or the restrictions imposed by Part 164 of Title 45 of the Code of Federal Regulations, including the manipulation of the information in any way that might reveal individually identifiable medical information. (B) For purposes of this paragraph, Section 1374.8 of the Health and Safety Code shall not apply. (22) Information may be disclosed pursuant to subdivision (a) of Section 15633.5 of the Welfare and Institutions Code by a person required to make a report pursuant to Section 15630 of the Welfare and Institutions Code, provided that the disclosure under subdivision (a) of Section 15633.5 concerns a report made by that person. Covered entities, as they are defined in Section 160.103 of Title 45 of the Code of Federal Regulations, shall comply with the requirements of the Health Insurance Portability and Accountability Act (HIPAA) privacy rule pursuant to subsection (c) of Section 164.512 of Title 45 of the Code of Federal Regulations if the disclosure is not for the purpose of public health surveillance, investigation, intervention, or reporting an injury or death. (d) Except to the extent expressly authorized by a patient, enrollee, or subscriber, or as provided by subdivisions (b) and (c), a provider of health care, health care service plan, contractor, or corporation and its subsidiaries and affiliates shall not intentionally share, sell, use for marketing, or otherwise use medical information for a purpose not necessary to provide health care services to the patient. (e) Except to the extent expressly authorized by a patient or enrollee or subscriber or as provided by subdivisions (b) and (c), a contractor or corporation and its subsidiaries and affiliates shall not further disclose medical information regarding a patient of the provider of health care or an enrollee or subscriber of a health care service plan or insurer or self-insured employer received under this section to a person or entity that is not engaged in providing direct health care services to the patient or his or her provider of health care or health care service plan or insurer or self-insured employer.

56.1007. (a) A provider of health care, health care service plan, or contractor may, in accordance with subdivision (c) or (d), disclose to a family member, other relative, domestic partner, or a close

personal friend of the patient, or any other person identified by the patient, the medical information directly relevant to that person's involvement with the patient's care or payment related to the patient's health care.

(b) A provider of health care, health care service plan, or contractor may use or disclose medical information to notify, or assist in the notification of, including identifying or locating, a family member, a personal representative of the patient, a domestic partner, or another person responsible for the care of the patient of the patient's location, general condition, or death. Any use or disclosure of medical information for those notification purposes shall be in accordance with the provisions of subdivision (c), (d), or (e), as applicable.

(c) (1) Except as provided in paragraph (2), if the patient is present for, or otherwise available prior to, a use or disclosure permitted by subdivision (a) or (b) and has the capacity to make health care decisions, the provider of health care, health care service plan, or contractor may use or disclose the medical information if it does any of the following:

(A) Obtains the patient's agreement. (B) Provides the patient with the opportunity to object to the disclosure, and the patient does not express an objection. (C) Reasonably infers from the circumstances, based on the exercise of professional judgment that the patient does not object to the disclosure. (2) A provider of health care who is a psychotherapist, as defined in Section 1010 of the Evidence Code, may use or disclose medical information pursuant to this subdivision only if the psychotherapist complies with subparagraph (A) or (B) of paragraph (1).

(d) If the patient is not present, or the opportunity to agree or object to the use or disclosure cannot practicably be provided because of the patient's incapacity or an emergency circumstance, the provider of health care, health care service plan, or contractor may, in the exercise of professional judgment, determine whether the disclosure is in the best interests of the patient and, if so, disclose only the medical information that is directly relevant to the person's involvement with the patient's health care. A provider of health care, health care service plan, or contractor may use professional judgment and its experience with common practice to make reasonable inferences of the patient's best interest in allowing a person to act on behalf of the patient to pick up filled prescriptions, medical supplies, X-rays, or other similar forms of medical information.

(e) A provider of health care, health care service plan, or contractor may use or disclose medical information to a public or private entity authorized by law or by its charter to assist in disaster relief efforts, for the purpose of coordinating with those entities the uses or disclosures permitted by subdivision (b). The requirements in subdivisions (c) and (d) apply to those uses and disclosures to the extent that the provider of health care, health care service plan, or contractor, in the exercise of professional judgment, determines that the requirements do not interfere with the ability to respond to the emergency circumstances.

(f) Nothing in this section shall be construed to interfere with or limit the access authority of Protection and Advocacy, Inc., the Office of Patients' Rights, or any county patients' rights advocates to access medical information pursuant to any state or federal law.

56.101. (a) Every provider of health care, health care service plan, pharmaceutical company, or contractor who creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information shall do so in a manner that preserves the confidentiality of the information contained therein. Any provider of health care, health care service plan, pharmaceutical company, or contractor who negligently creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information shall be subject to the remedies and penalties provided under subdivisions (b) and (c) of Section 56.36.

(b) (1) An electronic health record system or electronic medical record system shall do the

following: (A) Protect and preserve the integrity of electronic medical information. (B) Automatically record and preserve any change or deletion of any electronically stored medical information. The record of any change or deletion shall include the identity of the person who accessed and changed the medical information, the date and time the medical information was accessed, and the change that was made to the medical information. (2) A patient's right to access or receive a copy of his or her electronic medical records upon request shall be consistent with applicable state and federal laws governing patient access to, and the use and disclosures of, medical information. (c) This section shall apply to an "electronic medical record" or "electronic health record" that meets the definition of "electronic health record," as that term is defined in Section 17921(5) of Title 42 of the United States Code. 56.102. (a) A pharmaceutical company may not require a patient, as a condition of receiving pharmaceuticals, medications, or prescription drugs, to sign an authorization, release, consent, or waiver that would permit the disclosure of medical information that otherwise may not be disclosed under Section 56.10 or any other provision of law, unless the disclosure is for one of the following purposes: (1) Enrollment of the patient in a patient assistance program or prescription drug discount program. (2) Enrollment of the patient in a clinical research project. (3) Prioritization of distribution to the patient of a prescription medicine in limited supply in the United States. (4) Response to an inquiry from the patient communicated in writing, by telephone, or by electronic mail. (b) Except as provided in subdivision (a) or Section 56.10, a pharmaceutical company may not disclose medical information provided to it without first obtaining a valid authorization from the patient.

56.103. (a) A provider of health care may disclose medical information to a county social worker, a probation officer, or any other person who is legally authorized to have custody or care of a minor for the purpose of coordinating health care services and medical treatment provided to the minor. (b) For purposes of this section, health care services and medical treatment includes one or more providers of health care providing, coordinating, or managing health care and related services, including, but not limited to, a provider of health care coordinating health care with a third party, consultation between providers of health care and medical treatment relating to a minor, or a provider of health care referring a minor for health care services to another provider of health care. (c) For purposes of this section, a county social worker, a probation officer, or any other person who is legally authorized to have custody or care of a minor shall be considered a third party who may receive any of the following: (1) Medical information described in Sections 56.05 and 56.10. (2) Protected health information described in Section 160.103 of Title 45 of the Code of Federal Regulations. (d) Medical information disclosed to a county social worker, probation officer, or any other person who is legally authorized to have custody or care of a minor shall not be further disclosed by the recipient unless the disclosure is for the purpose of coordinating health care services and medical treatment of the minor and the disclosure is authorized by law. Medical information disclosed pursuant to this section may not be admitted into evidence in any criminal or delinquency proceeding against the minor. Nothing in this subdivision shall prohibit identical evidence from being admissible in a criminal proceeding if that evidence is derived solely from lawful means other than this section and is permitted by law. (e) (1) Notwithstanding Section 56.104, if a provider of health care determines that the disclosure of medical information concerning the diagnosis and treatment of a mental health condition of a minor is reasonably necessary for the purpose of assisting in coordinating the treatment and care of the minor, that information may be disclosed to a county social worker, probation officer, or any

other person who is legally authorized to have custody or care of the minor. The information shall not be further disclosed by the recipient unless the disclosure is for the purpose of coordinating mental health services and treatment of the minor and the disclosure is authorized by law. (2) As used in this subdivision, "medical information" does not include psychotherapy notes as defined in Section 164.501 of Title 45 of the Code of Federal Regulations.

(f) The disclosure of information pursuant to this section is not intended to limit the disclosure of information when that disclosure is otherwise required by law.

(g) For purposes of this section, "minor" means a minor taken into temporary custody or as to who a petition has been filed with the court, or who has been adjudged to be a dependent child or ward of the juvenile court pursuant to Section 300 or 601 of the Welfare and Institutions Code.

(h) (1) Except as described in paragraph (1) of subdivision (e), nothing in this section shall be construed to limit or otherwise affect existing privacy protections provided for in state or federal law (2) Nothing in this section shall be construed to expand the authority of a social worker, probation officer, or custodial caregiver beyond the authority provided under existing law to a parent or a patient representative regarding access to medical information.

56.104. (a) Notwithstanding subdivision (c) of Section 56.10, except as provided in subdivision (e), no provider of health care, health care service plan, or contractor may release medical information to persons or entities who have requested that information and who are authorized by law to receive that information pursuant to subdivision (c) of Section 56.10, if the requested information specifically relates to the patient's participation in outpatient treatment with a psychotherapist, unless the person or entity requesting that information submits to the patient pursuant to subdivision (b) and to the provider of health care, health care service plan, or contractor a written request, signed by the person requesting the information or an authorized agent of the entity requesting the information, that includes all of the following: (1) The specific information relating to a patient's participation in outpatient treatment with a psychotherapist being requested and its specific intended use or uses. (2) The length of time during which the information will be kept before being destroyed or disposed of. A person or entity may extend that timeframe, provided that the person or entity notifies the provider, plan, or contractor of the extension. Any notification of an extension shall include the specific reason for the extension, the intended use or uses of the information during the extended time, and the expected date of the destruction of the information. (3) A statement that the information will not be used for any purpose other than its intended use. (4) A statement that the person or entity requesting the information will destroy the information and all copies in the person's or entity's possession or control, will cause it to be destroyed, or will return the information and all copies of it before or immediately after the length of time specified in paragraph (2) has expired.

(b) The person or entity requesting the information shall submit a copy of the written request required by this section to the patient within 30 days of receipt of the information requested, unless the patient has signed a written waiver in the form of a letter signed and submitted by the patient to the provider of health care or health care service plan waiving notification.

(c) For purposes of this section, "psychotherapist" means a person who is both a "psychotherapist" as defined in Section 1010 of the Evidence Code and a "provider of health care" as defined in Section 56.05.

(d) This section does not apply to the disclosure or use of medical information by a law enforcement agency or a regulatory agency when required for an investigation of unlawful activity

or for licensing, certification, or regulatory purposes, unless the disclosure is otherwise prohibited by law.

(e) This section shall not apply to any of the following: (1) Information authorized to be disclosed pursuant to paragraph (1) of subdivision (c) of Section 56.10. (2) Information requested from a psychotherapist by law enforcement or by the target of the threat subsequent to a disclosure by that psychotherapist authorized by paragraph (19) of subdivision (c) of Section 56.10, in which the additional information is clearly necessary to prevent the serious and imminent threat disclosed under that paragraph. (3) Information disclosed by a psychotherapist pursuant to paragraphs (14) and (22) of subdivision (c) of Section 56.10 and requested by an agency investigating the abuse reported pursuant to those paragraphs.

(f) Nothing in this section shall be construed to grant any additional authority to a provider of health care, health care service plan, or contractor to disclose information to a person or entity without the patient's consent.

56.105. Whenever, prior to the service of a complaint upon a defendant in any action arising out of the professional negligence of a person holding a valid physician's and surgeon's certificate issued pursuant to Chapter 5 (commencing with Section 2000) of Division 2 of the Business and Professions Code, or a person holding a valid license as a marriage and family therapist issued pursuant to Chapter 13 (commencing with Section 4980) of Division 2 of the Business and Professions Code, a demand for settlement or offer to compromise is made on a patient's behalf, the demand or offer shall be accompanied by an authorization to disclose medical information to persons or organizations insuring, responsible for, or defending professional liability that the certificate holder may incur. The authorization shall be in accordance with Section 56.11 and shall authorize disclosure of that information that is necessary to investigate issues of liability and extent of potential damages in evaluating the merits of the demand for settlement or offer to compromise. Notice of any request for medical information made pursuant to an authorization as provided by this section shall be given to the patient or the patient's legal representative. The notice shall describe the inclusive subject matter and dates of the materials requested and shall also authorize the patient or the patient's legal representative to receive, upon request, copies of the information at his or her expense. Nothing in this section shall be construed to waive or limit any applicable privileges set forth in the Evidence Code except for the disclosure of medical information subject to the patient's authorization. Nothing in this section shall be construed as authorizing a representative of any person from whom settlement has been demanded to communicate in violation of the physician-patient privilege with a treating physician, or to communicate in violation of the psychotherapist-patient privilege with a treating licensed marriage and family therapist, except for the medical information request.

The requirements of this section are independent of the requirements of Section 364 of the Code of Civil Procedure.

56.106. (a) Notwithstanding Section 3025 of the Family Code, paragraph (2) of subdivision (c) of Section 56.11, or any other provision of law, a psychotherapist who knows that a minor has been removed from the custody of his or her parent or guardian pursuant to Article 6 (commencing with Section 300) to Article 10 (commencing with Section 360), inclusive, of Chapter 2 of Part 1 of Division 2 of the Welfare and Institutions Code shall not release the mental health records of the minor patient and shall not disclose mental health information about that minor patient based upon an authorization to release those records signed by the minor's parent or guardian. This restriction

shall not apply if the juvenile court has issued an order authorizing the parent or guardian to sign an authorization for the release of the mental health records or the information about the minor patient after finding that such an order would not be detrimental to the minor patient.

(b) For purposes of this section, the following definitions apply: (1) "Mental health records" means mental health records as defined by subdivision (b) of Section 123105 of the Health and Safety Code. (2) "Psychotherapist" means a provider of health care as defined in Section 1010 of the Evidence Code.

(c) When the juvenile court has issued an order authorizing the parent or guardian to sign an authorization for the release of the mental health records or information about that minor patient under the circumstances described in subdivision (a), the parent or guardian seeking the release of the minor's records or information about the minor shall present a copy of the court order to the psychotherapist before any records or information may be released pursuant to the signed authorization.

(d) Nothing in this section shall be construed to prevent or limit a psychotherapist's authority under subdivision (a) of Section 123115 of the Health and Safety Code to deny a parent's or guardian's written request to inspect or obtain copies of the minor patient's mental health records, notwithstanding the fact that the juvenile court has issued an order authorizing the parent or guardian to sign an authorization for the release of the mental health records or information about that minor patient. Liability for a psychotherapist's decision not to release the mental health records of the minor patient or not to disclose information about the minor patient pursuant to the authority of subdivision (a) of Section 123115 of the Health and Safety Code shall be governed by that section.

(e) Nothing in this section shall be construed to impose upon a psychotherapist a duty to inquire or investigate whether a child has been removed from the physical custody of his or her parent or guardian pursuant to Article 6 (commencing with Section 300) to Article 10 (commencing with Section 360), inclusive, of Chapter 2 of Part 1 of Division 2 of the Welfare and Institutions Code when a parent or guardian presents the minor's psychotherapist with an authorization to release information or the mental health records regarding the minor patient.

56.107. (a) Notwithstanding any other law, and to the extent permitted by federal law, a health care service plan shall take the following steps to protect the confidentiality of a subscriber's or enrollee's medical information on and after January 1, 2015: (1) A health care service plan shall permit subscribers and enrollees to request, and shall accommodate requests for, communication in the form and format requested by the individual, if it is readily producible in the requested form and format, or at alternative locations, if the subscriber or enrollee clearly states either that the communication discloses medical information or provider name and address relating to receipt of sensitive services or that disclosure of all or part of the medical information or provider name and address could endanger the subscriber or enrollee. (2) A health care service plan may require the subscriber or enrollee to make a request for a confidential communication described in paragraph (1), in writing or by electronic transmission. (3) A health care service plan may require that a confidential communications request contain a statement that the request pertains to either medical information related to the receipt of sensitive services or that disclosure of all or part of the medical information could endanger the subscriber or enrollee. The health care service plan shall not require an explanation as to the basis for a subscriber's or enrollee's statement that disclosure could endanger the subscriber or enrollee. (4) The confidential communication request shall be valid until the subscriber or enrollee submits a revocation of the request or a new confidential

communication request is submitted. (5) For the purposes of this section, a confidential communications request shall be implemented by the health care service plan within seven calendar days of receipt of an electronic transmission or telephonic request or within 14 calendar days of receipt by first-class mail. The health care service plan shall acknowledge receipt of the confidential communications request and advise the subscriber or enrollee of the status of implementation of the request if a subscriber or enrollee contacts the health care service plan.

(b) Notwithstanding subdivision (a), the provider of health care may make arrangements with the subscriber or enrollee for the payment of benefit cost sharing and communicate that arrangement with the health care service plan.

(c) A health care service plan shall not condition enrollment or coverage on the waiver of rights provided in this section.

56.11. Any person or entity that wishes to obtain medical information pursuant to subdivision (a) of Section 56.10, other than a person or entity authorized to receive medical information pursuant to subdivision (b) or (c) of Section 56.10, except as provided in paragraph (21) of subdivision (c) of Section 56.10, shall obtain a valid authorization for the release of this information. An authorization for the release of medical information by a provider of health care, health care service plan, pharmaceutical company, or contractor shall be valid if it: (a) Is handwritten by the person who signs it or is in a typeface no smaller than 14-point type. (b) Is clearly separate from any other language present on the same page and is executed by a signature which serves no other purpose than to execute the authorization. (c) Is signed and dated by one of the following: (1) The patient. A patient who is a minor may only sign an authorization for the release of medical information obtained by a provider of health care, health care service plan, pharmaceutical company, or contractor in the course of furnishing services to which the minor could lawfully have consented under Part 1 (commencing with Section 25) or Part 2.7 (commencing with Section 60). (2) The legal representative of the patient, if the patient is a minor or an incompetent. However, authorization may not be given under this subdivision for the disclosure of medical information obtained by the provider of health care, health care service plan, pharmaceutical company, or contractor in the course of furnishing services to which a minor patient could lawfully have consented under Part 1 (commencing with Section 25) or Part 2.7 (commencing with Section 60). (3) The spouse of the patient or the person financially responsible for the patient, where the medical information is being sought for the sole purpose of processing an application for health insurance or for enrollment in a nonprofit hospital plan, a health care service plan, or an employee benefit plan, and where the patient is to be an enrolled spouse or dependent under the policy or plan. (4) The beneficiary or personal representative of a deceased patient. (d) States the specific uses and limitations on the types of medical information to be disclosed. (e) States the name or functions of the provider of health care, health care service plan, pharmaceutical company, or contractor that may disclose the medical information. (f) States the name or functions of the persons or entities authorized to receive the medical information. (g) States the specific uses and limitations on the use of the medical information by the persons or entities authorized to receive the medical information. (h) States a specific date after which the provider of health care, health care service plan, pharmaceutical company, or contractor is no longer authorized to disclose the medical information. (i) Advises the person signing the authorization of the right to receive a copy of the authorization.

56.12. Upon demand by the patient or the person who signed an authorization, a provider of health care, health care service plan, pharmaceutical company, or contractor possessing the authorization shall furnish a true copy thereof.

56.13. A recipient of medical information pursuant to an authorization as provided by this chapter or pursuant to the provisions of subdivision (c) of Section 56.10 may not further disclose that medical information except in accordance with a new authorization that meets the requirements of Section 56.11, or as specifically required or permitted by other provisions of this chapter or by law.

56.14. A provider of health care, health care service plan, or contractor that discloses medical information pursuant to the authorizations required by this chapter shall communicate to the person or entity to which it discloses the medical information any limitations in the authorization regarding the use of the medical information. No provider of health care, health care service plan, or contractor that has attempted in good faith to comply with this provision shall be liable for any unauthorized use of the medical information by the person or entity to which the provider, plan, or contractor disclosed the medical information.

56.15. Nothing in this part shall be construed to prevent a person who could sign the authorization pursuant to subdivision (c) of Section 56.11 from cancelling or modifying an authorization. However, the cancellation or modification shall be effective only after the provider of health care actually receives written notice of the cancellation or modification.

56.16. For disclosures not addressed by Section 56.1007, unless there is a specific written request by the patient to the contrary, nothing in this part shall be construed to prevent a general acute care hospital, as defined in subdivision (a) of Section 1250 of the Health and Safety Code, upon an inquiry concerning a specific patient, from releasing at its discretion any of the following information: the patient's name, address, age, and sex; a general description of the reason for treatment (whether an injury, a burn, poisoning, or some unrelated condition); the general nature of the injury, burn, poisoning, or other condition; the general condition of the patient; and any information that is not medical information as defined in Section 56.05.

IDENTITY THEFT

PENAL CODE – PEN

PART 1. OF CRIMES AND PUNISHMENTS [25 - 680] (Part 1 enacted 1872.)

TITLE 13. OF CRIMES AGAINST PROPERTY [450 - 593g] (Title 13 enacted 1872.)

CHAPTER 8. False Personation and Cheats [528 - 539] (Chapter 8 enacted 1872.)

530.5.

(a) Every person who willfully obtains personal identifying information, as defined in subdivision (b) of Section 530.55, of another person, and uses that information for any unlawful purpose, including to obtain, or attempt to obtain, credit, goods, services, real property, or medical information without the consent of that person, is guilty of a public offense, and upon conviction therefor, shall be punished by a fine, by imprisonment in a county jail not to exceed one year, or by both a fine and imprisonment, or by imprisonment pursuant to subdivision (h) of Section 1170.

(b) In any case in which a person willfully obtains personal identifying information of another

person, uses that information to commit a crime in addition to a violation of subdivision (a), and is convicted of that crime, the court records shall reflect that the person whose identity was falsely used to commit the crime did not commit the crime.

(c) (1) Every person who, with the intent to defraud, acquires or retains possession of the personal identifying information, as defined in subdivision (b) of Section 530.55, of another person is guilty of a public offense, and upon conviction therefor, shall be punished by a fine, by imprisonment in a county jail not to exceed one year, or by both a fine and imprisonment. (2) Every person who, with the intent to defraud, acquires or retains possession of the personal identifying information, as defined in subdivision (b) of Section 530.55, of another person, and who has previously been convicted of a violation of this section, upon conviction therefor shall be punished by a fine, by imprisonment in a county jail not to exceed one year, or by both a fine and imprisonment, or by imprisonment pursuant to subdivision (h) of Section 1170. (3) Every person who, with the intent to defraud, acquires or retains possession of the personal identifying information, as defined in subdivision (b) of Section 530.55, of 10 or more other persons is guilty of a public offense, and upon conviction therefor, shall be punished by a fine, by imprisonment in a county jail not to exceed one year, or by both a fine and imprisonment, or by imprisonment pursuant to subdivision (h) of Section 1170.

(d) (1) Every person who, with the intent to defraud, sells, transfers, or conveys the personal identifying information, as defined in subdivision (b) of Section 530.55, of another person is guilty of a public offense, and upon conviction therefor, shall be punished by a fine, by imprisonment in a county jail not to exceed one year, or by both a fine and imprisonment, or by imprisonment pursuant to subdivision (h) of Section 1170. (2) Every person who, with actual knowledge that the personal identifying information, as defined in subdivision (b) of Section 530.55, of a specific person will be used to commit a violation of subdivision (a), sells, transfers, or conveys that same personal identifying information is guilty of a public offense, and upon conviction therefor, shall be punished by a fine, by imprisonment pursuant to subdivision (h) of Section 1170, or by both a fine and imprisonment.

(e) Every person who commits mail theft, as defined in Section 1708 of Title 18 of the United States Code, is guilty of a public offense, and upon conviction therefor shall be punished by a fine, by imprisonment in a county jail not to exceed one year, or by both a fine and imprisonment. Prosecution under this subdivision shall not limit or preclude prosecution under any other provision of law, including, but not limited to, subdivisions (a) to (c), inclusive, of this section.

(f) An interactive computer service or access software provider, as defined in subsection (f) of Section 230 of Title 47 of the United States Code, shall not be liable under this section unless the service or provider acquires, transfers, sells, conveys, or retains possession of personal information with the intent to defraud.

(Amended by Stats. 2011, Ch. 15, Sec. 383. Effective April 4, 2011. Operative October 1, 2011, by Sec. 636 of Ch. 15, as amended by Stats. 2011, Ch. 39, Sec. 68.)

530.6.

(a) A person who has learned or reasonably suspects that his or her personal identifying information has been unlawfully used by another, as described in subdivision (a) of Section 530.5, may initiate a law enforcement investigation by contacting the local law enforcement agency that has jurisdiction over his or her actual residence or place of business, which shall take a police report of the matter, provide the complainant with a copy of that report, and begin an investigation of the facts. If the suspected crime was committed in a different jurisdiction, the local law

enforcement agency may refer the matter to the law enforcement agency where the suspected crime was committed for further investigation of the facts.

(b) A person who reasonably believes that he or she is the victim of identity theft may petition a court, or the court, on its own motion or upon application of the prosecuting attorney, may move, for an expedited judicial determination of his or her factual innocence, where the perpetrator of the identity theft was arrested for, cited for, or convicted of a crime under the victim's identity, or where a criminal complaint has been filed against the perpetrator in the victim's name, or where the victim's identity has been mistakenly associated with a record of criminal conviction. Any judicial determination of factual innocence made pursuant to this section may be heard and determined upon declarations, affidavits, police reports, or other material, relevant, and reliable information submitted by the parties or ordered to be part of the record by the court. Where the court determines that the petition or motion is meritorious and that there is no reasonable cause to believe that the victim committed the offense for which the perpetrator of the identity theft was arrested, cited, convicted, or subject to a criminal complaint in the victim's name, or that the victim's identity has been mistakenly associated with a record of criminal conviction, the court shall find the victim factually innocent of that offense. If the victim is found factually innocent, the court shall issue an order certifying this determination.

(c) After a court has issued a determination of factual innocence pursuant to this section, the court may order the name and associated personal identifying information contained in court records, files, and indexes accessible by the public deleted, sealed, or labeled to show that the data is impersonated and does not reflect the defendant's identity.

(d) A court that has issued a determination of factual innocence pursuant to this section may at any time vacate that determination if the petition, or any information submitted in support of the petition, is found to contain any material misrepresentation or fraud.

(e) The Judicial Council of California shall develop a form for use in issuing an order pursuant to this section.

(f) For purposes of this section, "person" means a natural person, firm, association, organization, partnership, business trust, company, corporation, limited liability company, or public entity.

(Amended by Stats. 2006, Ch. 10, Sec. 2. Effective February 25, 2006.)

530.7.

(a) In order for a victim of identity theft to be included in the data base established pursuant to subdivision (c), he or she shall submit to the Department of Justice a court order obtained pursuant to any provision of law, a full set of fingerprints, and any other information prescribed by the department.

(b) Upon receiving information pursuant to subdivision (a), the Department of Justice shall verify the identity of the victim against any driver's license or other identification record maintained by the Department of Motor Vehicles.

(c) The Department of Justice shall establish and maintain a data base of individuals who have been victims of identity theft. The department shall provide a victim of identity theft or his or her authorized representative access to the data base in order to establish that the individual has been a victim of identity theft. Access to the data base shall be limited to criminal justice agencies, victims of identity theft, and individuals and agencies authorized by the victims.

(d) The Department of Justice shall establish and maintain a toll-free telephone number to provide access to information under subdivision (c).

(e) This section shall be operative September 1, 2001.

(Amended by Stats. 2001, Ch. 854, Sec. 30. Effective January 1, 2002.)

COMMUNICABLE DISEASE REPORTING REQUIREMENTS

Title 17. California Code of Regulations, §2500

Reportable Disease & Conditions

DISEASE REPORTING LAWS

17 CCR § 2500

§ 2500. Reporting to the Local Health Authority.

(a) The following definitions shall govern the interpretation of this Subchapter.(1) 'CDC' means the Centers for Disease Control and Prevention, United States Department of Health and Human Services.(2) 'CSTE' means the Council of State and Territorial Epidemiologists.(3) 'MMWR' means the Morbidity and Mortality Weekly Report.(4) 'Acute HIV infection' means detectable HIV-1 RNA or p24 antigen in serum or plasma in the setting of a negative or indeterminate HIV-1 antibody test result for patients tested using a currently approved HIV test algorithm, as defined in section 2641.57.(5) 'Case' means (A) a person who has been diagnosed by a health care provider, who is lawfully authorized to diagnose, using clinical judgment or laboratory evidence, to have a particular disease or condition listed in subsection (j); or (B) a person who meets the definition of a case in Section 2564 - Diarrhea of the Newborn, Section 2574 - Food Poisoning, Section 2612 Salmonella Infections (Other than Typhoid Fever), Section 2628 - Typhoid Fever, or Section 2636 - Venereal Disease; or (C) a person who is considered a case of a disease or condition that satisfies the most recent communicable disease surveillance case definitions established by the CDC and published in the Morbidity and Mortality Weekly Report (MMWR) or its supplements; or (D) an animal that has been determined, by a person authorized to do so, to have rabies or plague; or (E) a person who has been diagnosed with HIV infection using a currently approved HIV test algorithm, as defined in section 2641.57.(6) 'Clinical signs' means the objective evidence of disease.(7) 'Clinical symptoms' means the subjective sensation of disease felt by the patient.(8) 'Communicable disease' means an illness due to a specific microbiological or parasitic agent or its toxic products which arises through transmission of that agent or its products from an infected person, animal, or inanimate reservoir to a susceptible host, either directly or indirectly through an intermediate plant or animal host, vector, or the inanimate environment.(9) 'Director' means State Director of Public Health.(10) 'Drug susceptibility testing' means the process where at least one isolate from a culture of a patient's specimen is subjected to antimicrobial testing to determine if growth is inhibited by drugs commonly used to treat such infections.(11) 'Epidemiological risk factors' means those attributes, behaviors, exposures, or other factors that alter the probability of disease.(12) 'Epidemiologically linked case' means a case in which the patient has/had contact with one or more persons who have/had the disease, and transmission of the agent by the usual modes of transmission is plausible.(13) 'Foodborne disease' means illness suspected by a health care provider to have resulted from consuming a contaminated food.(14) 'Foodborne disease outbreak' means an incident in which two or more persons experience a similar illness after ingestion of a common food, and epidemiologic analysis implicates the food as the source of the illness. There are two exceptions: even one case of botulism or chemical poisoning constitutes an outbreak if laboratory studies identify the causative agent in the food.(15) 'Health care provider' means a physician and surgeon, a veterinarian, a podiatrist, a nurse practitioner, a physician assistant, a registered nurse, a nurse midwife, a school nurse, an infection control practitioner, a medical examiner, a coroner, or a dentist.(16) 'Health officer' and 'local health officer' as used in this subchapter includes county, city,

and district health officers.(17) 'In attendance' means the existence of the relationship whereby a health care provider renders those services which are authorized by the health care provider's licensure or certification.(18) 'Infection control practitioner' means any person designated by a hospital, nursing home, clinic, or other health care facility as having responsibilities which include the detection, reporting, control and prevention of infections within the institution.(19) 'Laboratory findings' means (A) the results of a laboratory examination of any specimen derived from the human body which yields microscopical, cultural, immunological, serological, or other evidence suggestive of a disease or condition made reportable by these regulations; or (B) the results of a laboratory examination of any specimen derived from an animal which yields evidence of rabies or plague.(20) 'Multidrug-resistant *Mycobacterium tuberculosis*' means a laboratory culture or subculture of *Mycobacterium tuberculosis* which is determined by antimicrobial susceptibility testing to be resistant to at least isoniazid and rifampin.(21) 'Pandemic potential' means the potential ability of a pathogen to spread easily and efficiently in the human population, crossing international boundaries, and usually affecting many people. Such pathogens may be associated with severe illness and death.(22) 'Outbreak' means the occurrence of cases of a disease (illness) above the expected or baseline level, usually over a given period of time, in a geographic area or facility, or in a specific population group. The number of cases indicating the presence of an outbreak will vary according to the disease agent, size and type of population exposed, previous exposure to the agent, and the time and place of occurrence. Thus, the designation of an outbreak is relative to the usual frequency of the disease in the same facility or community, among the specified population, over a comparable period of time. A single case of a communicable disease long absent from a population or the first invasion by a disease not previously recognized requires immediate reporting and epidemiologic investigation.(23) 'Personal information' means any information that identifies or describes a person, including, but not limited to, his or her name, social security number, date of birth, physical description, home address, home telephone number, and medical or employment history.(24) 'Sexually Transmitted Diseases' means Chancroid, Lymphogranuloma Venereum, Granuloma Inguinale, Syphilis, Gonorrhea, Chlamydia, and Nongonococcal Urethritis.(25) 'Suspected case' means (A) a person whom a health care provider believes, after weighing signs, symptoms, and/or laboratory evidence, to probably have a particular disease or condition listed in subsection (j); or (B) a person who is considered a probable case, or an epidemiologically-linked case, or who has supportive laboratory findings under the most recent communicable disease surveillance case definition established by CDC and published in the Morbidity and Mortality Weekly Report (MMWR) or its supplements; or (C) an animal which has been determined by a veterinarian to exhibit clinical signs or which has laboratory findings suggestive of rabies or plague.(26) 'Unusual disease' means a rare disease or a newly apparent or emerging disease or syndrome of uncertain etiology which a health care provider has reason to believe could possibly be caused by a transmissible infectious agent or microbial toxin.(27) 'Waterborne disease outbreak' means an incident in which two or more persons experienced a similar illness after consumption or use of the same water intended for drinking or after water contact such as by immersion, and epidemiologic investigation by public health authorities implicates the same water as the source of the waterborne illness. There is one exception: a single case of waterborne chemical poisoning constitutes an outbreak if laboratory studies indicate that the source water is contaminated by the chemical.

(b) It shall be the duty of every health care provider, knowing of or in attendance on a case or suspected case of any of the diseases or conditions listed in subsection (j) of this section, to report to the local health officer for the jurisdiction where the patient resides as required in subsection (h)

of this section. Where no health care provider is in attendance, any individual having knowledge of a person who is suspected to be suffering from one of the diseases or conditions listed in subsection (j) of this section may make such a report to the local health officer for the jurisdiction where the patient resides.

(c) The administrator of each health facility, clinic or other setting where more than one health care provider may know of a case, a suspected case or an outbreak of disease within the facility shall establish and be responsible for administrative procedures to assure that reports are made to the local health officer.

(d) Each report made pursuant to subsection (b) shall include all of the following information if known: (1) name of the disease or condition being reported; the date of onset; the date of diagnosis; the name, address, telephone number, occupation, race/ethnic group, Social Security number, sex, age, and date of birth for the case or suspected case; the date of death if death has occurred; and the name, address and telephone number of the person making the report. (2) If the disease reported pursuant to subsection (b) is hepatitis, a sexually transmitted disease or tuberculosis, then the report shall include the following applicable information, if known: (A) hepatitis information as to the type of hepatitis, type-specific laboratory findings, and sources of exposure, (B) sexually transmitted disease information as to the specific causative agent, syphilis-specific laboratory findings, and any complications of gonorrhea or chlamydia infections, or (C) tuberculosis information on the diagnostic status of the case or suspected case, bacteriologic, radiologic and tuberculin skin test findings, information regarding the risk of transmission of the disease to other persons, and a list of the anti-tuberculosis medications administered to the patient.

(e) Confidential Morbidity Report forms, are available from the local health department for reporting as required by this section.

(f) Information reported pursuant to this section is acquired in confidence and shall not be disclosed by the local health officer except as authorized by these regulations, as required by state or federal law, or with the written consent of the individual to whom the information pertains or the legal representative of the individual.

(g) Upon the State Department of Public Health's request, a local health department shall provide to the Department the information reported pursuant to this section. Absent the individual's written consent, no information that would directly or indirectly identify the case or suspected case as an individual who has applied for or been given services for alcohol or other drug abuse by a federally assisted drug or alcohol abuse treatment program (as defined in federal law at 42 C.F.R. Section 2.11) shall be included.

(h) The urgency of reporting is identified by symbols in the list of diseases and conditions in subsection (j) of this section. Those diseases with a diamond (<>) are considered emergencies and shall be reported immediately by telephone. Those diseases and conditions with a cross (+) shall be reported by mailing, telephoning, or electronically transmitting a report within one (1) working day of identification of the case or suspected case, except for acute HIV infection reporting which shall be reported by telephone (see (k) for specific requirements). Those diseases and conditions not otherwise identified by a diamond or a cross shall be reported by mailing a written report, telephoning, or electronically transmitting a report within seven (7) calendar days of the time of identification.

(i) For foodborne disease, the bullet (•) symbol indicates that, when two (2) or more cases or suspected cases of foodborne disease from separate households are suspected to have the same source of illness, they shall be reported immediately by telephone.

(j) Health care providers shall submit reports for the following diseases or conditions.

+	Amebiasis
	Anaplasmosis
<>	Anthrax, human or animal
+	Babesiosis
<>	Botulism (Infant, Foodborne, Wound, Other)
<>	Brucellosis, human
	Brucellosis, animal (except infections due to <i>Brucella canis</i>)
+	Campylobacteriosis
	Chancroid
+	Chickenpox (Varicella) (outbreaks, hospitalizations and deaths)
	<i>Chlamydia trachomatis</i> infections, including lymphogranuloma venereum (LGV)
<>	Cholera
<>	Ciguatera Fish Poisoning
+	Chikungunya virus infection
	Coccidioidomycosis
	Creutzfeldt-Jakob Disease (CJD) and other Transmissible Spongiform Encephalopathies (TSE)
+	Cryptosporidiosis Cyclosporiasis Cysticercosis or taeniasis
<>	Dengue virus infection
<>	Diphtheria
<>	Domoic Acid Poisoning (Amnesic Shellfish Poisoning)
	Ehrlichiosis
+	Encephalitis, Specify Etiology: Viral, Bacterial, Fungal, Parasitic
<>	<i>Escherichia coli</i> : shiga toxin producing (STEC) including <i>E. coli</i> O157
<>	Flavivirus infection of undetermined species
+	Foodborne Disease Giardiasis Gonococcal Infections
•	
+	<i>Haemophilus influenzae</i> , invasive disease, all serotypes (report an incident of less than five years of age)
+	Hantavirus Infections
<>	Hemolytic Uremic Syndrome
+	Hepatitis A, acute infection
	Hepatitis B (specify acute case or chronic)
	Hepatitis C (specify acute case or chronic)
	Hepatitis D (Delta) (specify acute case or chronic)
	Hepatitis E, acute infection
	Human Immunodeficiency Virus (HIV) infection, stage 3 (AIDS)
+	Human Immunodeficiency Virus (HIV), acute infection, (see (k) for additional reporting requirements)
	Influenza, deaths in laboratory-confirmed cases for ages 0-64 years
<>	Influenza, novel strains (human)
	Legionellosis
	Leprosy (Hansen Disease)
	Leptospirosis

+	Listeriosis
	Lyme Disease
+	Malaria
<>	Measles (Rubeola)
+	Meningitis, Specify Etiology: Viral, Bacterial, Fungal, Parasitic
<>	Meningococcal Infections
	Mumps
<>	Novel virus infection with pandemic potential
<>	Paralytic Shellfish Poisoning
+	Pertussis (Whooping Cough)
<>	Plague, human or animal
+	Poliovirus Infection
+	Psittacosis
+	Q Fever
<>	Rabies, human or animal
+	Relapsing Fever
	Respiratory syncytial virus (only report a death in a patient less than five years of age)
	Rickettsial Diseases (non-Rocky Mountain Spotted Fever), including Typhus and Typhus-like Illnesses
	Rocky Mountain Spotted Fever
	Rubella (German Measles)
	Rubella Syndrome, Congenital
+	Salmonellosis (Other than Typhoid Fever)
<>	Scombroid Fish Poisoning
<>	Shiga toxin (detected in feces)
+	Shigellosis
<>	Smallpox (Variola)
+	Streptococcal Infections (Outbreaks of Any Type and Individual Cases in Food Handlers and Dairy Workers Only)
+	Syphilis Tetanus
+	Trichinosis
+	Tuberculosis
<>	Tularemia, human
	Tularemia, animal
+	Typhoid Fever, Cases and Carriers
+	<i>Vibrio</i> Infections
<>	Viral Hemorrhagic Fevers, human or animal (e.g., Crimean- Congo, Ebola, Lassa and Marburg viruses)
+	West Nile virus infection
<>	Yellow Fever
+	Yersiniosis
<>	Zika virus infection
<>	OCCURRENCE of ANY UNUSUAL DISEASE

<> OUTBREAKS of ANY DISEASE (Including diseases not listed in Section 2500). Specify if institutional and/or open community.

(<>) = to be reported immediately by telephone.

(+) = to be reported by mailing a report, telephoning, or electronically transmitting a report within one (1) working day of identification of the case or suspected case.

(No diamond or cross symbol) = to be reported within seven (7) calendar days by mail, telephone, or electronic report from the time of identification.

(•) = when two (2) or more cases or suspected cases of foodborne disease from separate households are suspected to have the same source of illness, they should be reported immediately by telephone.

(k) In addition to routine reporting requirements set forth in section 2643.5, for acute HIV infection reporting, health care providers shall report all cases within one (1) working day to the local health officer of the jurisdiction in which the patient resides by telephone. If evidence of acute HIV infection is based on presence of HIV p24 antigen, providers shall not wait until HIV-1 RNA is detected before reporting to the local health officer.

Note: Authority cited: Sections 120130, 131050, 131051, 131052, 131080 and 131200, Health and Safety Code. Reference: Sections 1603.1, 100325, 103925, 113150, 113155, 120125, 120130, 120140, 120175, 120245, 120250, 131050, 131051 and 131080, Health and Safety Code; Sections 551, 554 and 555, Business and Professions Code; Section 1798.3, Civil Code; 42 C.F.R. Sections 2.11 and 2.12; Cal. Const., art. 1, Section 1; and Section 1040, Evidence Code.

California Health and Safety Code HIV/AIDS HIV Case (121022) and CD4 Reporting (121023)

121022.

(a) To ensure knowledge of current trends in the HIV epidemic and to ensure that California remains competitive for federal HIV and AIDS funding, health care providers and laboratories shall report cases of HIV infection to the local health officer using patient names. Local health officers shall report unduplicated HIV cases by name to the department.

(b) (1) Health care providers and local health officers shall submit cases of HIV infection pursuant to subdivision (a) by courier service, United States Postal Service express mail or registered mail, other traceable mail, person-to-person transfer, facsimile, or electronically by a secure and confidential electronic reporting system established by the department. (2) This subdivision shall be implemented using the existing resources of the department.

(c) The department and local health officers shall ensure continued reasonable access to anonymous HIV testing through alternative testing sites, as established by Section 120890, and in consultation with HIV planning groups and affected stakeholders, including representatives of persons living with HIV and health officers.

(d) The department shall promulgate emergency regulations to conform the relevant provisions of Article 3.5 (commencing with Section 2641.5) of Chapter 4 of Title 17 of the California Code of Regulations, consistent with this chapter, within one year of the effective date of this section.

(e) Pursuant to Section 121025, reported cases of HIV infection shall not be disclosed, discoverable, or compelled to be produced in any civil, criminal, administrative, or other proceeding.

(f) State and local health department employees and contractors shall be required to sign confidentiality agreements developed by the department that include information related to the penalties for a breach of confidentiality and the procedures for reporting a breach of confidentiality, prior to accessing confidential HIV-related public health records. Those agreements shall be reviewed annually by either the department or the appropriate local health department.

(g) No person shall disclose identifying information reported pursuant to subdivision (a) to the federal government, including, but not limited to, any agency, employee, agent, contractor, or anyone else acting on behalf of the federal government, except as permitted under subdivision (b) of Section 121025.

(h) (1) Any potential or actual breach of confidentiality of HIV-related public health records shall be investigated by the local health officer, in coordination with the department, when appropriate. The local health officer shall immediately report any evidence of an actual breach of confidentiality of HIV-related public health records at a city or county level to the department and the appropriate law enforcement agency. (2) The department shall investigate any potential or actual breach of confidentiality of HIV-related public health records at the state level, and shall report any evidence of such a breach of confidentiality to an appropriate law enforcement agency.

(i) Any willful, negligent, or malicious disclosure of cases of HIV infection reported pursuant to subdivision (a) shall be subject to the penalties prescribed in Section 121025.

(j) Nothing in this section shall be construed to limit other remedies and protections available under state or federal law. 121023. (a) Subject to subdivision (b), each clinical laboratory, as defined in Section 1206 of the Business and Professions Code, shall report all CD4+ T-Cell test results to the local health officer for the local health jurisdiction where the health care provider facility is located within seven days of the completion of the CD4+ T-Cell test. (b) A clinical laboratory shall not be required to report a CD4+ T-Cell test result, as required by this section, if the clinical laboratory can demonstrate that the CD4+ T-Cell test result is not related to a diagnosed case of HIV infection. (c) The clinical laboratory report with CD4+ T-Cell test results shall also include, if provided by the ordering health care provider, all of the following: (1) The patient's name. (2) The patient's date of birth. (3) The patient's gender. (4) The name, telephone number, and address of the local health care provider that ordered the test. (d) The clinical laboratory report with CD4+ T-Cell test results shall also include all of the following information: (1) CD4+ T-Cell test results expressed as an absolute count (the number of lymphocytes containing the CD4 epitope per cubic millimeter) and, if available, the relative count (the number of lymphocytes expressing the CD4 epitope as a percentage of total lymphocytes). (2) The type of laboratory test performed. (3) The date the laboratory test was performed. (4) The name, telephone number, and address of the clinical laboratory that performed the test. (5) The laboratory CLIA number. (6) The laboratory report number. (e) (1) Each local health officer shall inspect each clinical laboratory CD4+ T-Cell test report to determine if the test is related to a case of HIV infection. (2) If the clinical laboratory CD4+ T-Cell test result is related to a case of HIV infection, the local health officer shall report the case of HIV infection or AIDS, as appropriate, to the State Department of Public Health within 45 days of receipt of the laboratory report. (3) If the clinical laboratory CD4+ T-Cell test result is not related to a case of HIV infection, the local health officer shall destroy the laboratory CD4+ T-Cell test report. (f) Pursuant to Section 121025, CD4+ T-Cell test reports shall not be disclosed, discoverable, or compelled to be produced in any civil, criminal, administrative, or other proceeding. (g) CD4+ T-Cell test reports shall be considered confidential public health records as defined in Section 121035. (h) For the purposes of this section, "CD4+ T-Cell test" means any test used to measure the number of lymphocytes containing the CD4 epitope.

CALIFORNIA CODES HEALTH AND SAFETY CODE SECTION 120990

(a) Prior to ordering a test that identifies infection with HIV, a medical care provider shall inform the patient that the test is planned, provide information about the test, inform the patient that there are numerous treatment options available for a patient who tests positive for HIV and that a person who tests negative for HIV should continue to be routinely tested, and advise the patient that he or she has the right to decline the test. If a patient declines the test, the medical care provider shall note that fact in the patient's medical file.

(b) Subdivision (a) shall not apply when a person independently requests an HIV test from the provider.

(c) Except as provided in subdivision (a), no person shall administer a test for HIV infection unless the person being tested or his or her parent, guardian, conservator, or other person specified in Section 121020, signs a written statement documenting the person's informed consent to the test. This requirement does not apply to such a test performed at an alternative site pursuant to Sections 120890 or 120895. Nothing in this section shall be construed to allow a person to administer a test for HIV unless that person is otherwise permitted under current law to administer an HIV test

(d) Nothing in this section shall preclude a medical examiner or other physician from ordering or performing a test to detect HIV on a cadaver when an autopsy is performed or body parts are donated pursuant to the Uniform Anatomical Gift Act (Chapter 3.5 (commencing with Section 7150) of Part 1 of Division 7).

(e) (1) The requirements of subdivision (c) do not apply when blood is tested as part of a scientific investigation conducted either by a medical researcher operating under the approval of an institutional review board or by the department, in accordance with a protocol for unlinked testing.

(2) For purposes of this subdivision, "unlinked testing" means blood samples that are obtained anonymously, or that have the name or identifying information of the individual who provided the sample removed in a manner that prevents the test results from ever being linked to a particular individual who participated in the research or study.

(f) Nothing in this section shall be construed to permit any person to unlawfully disclose an individual's HIV status, or to otherwise violate provisions of Section 54 of the Civil Code, the Americans With Disabilities Act of 1990 (Public Law 101-336), or the California Fair Employment and Housing Act (Part 2.8 (commencing with Section 12900) of Division 3 of Title 2 of the Government Code), which prohibit discrimination against individuals who are living with HIV, or who test positive for HIV, or are presumed to be HIV-positive.

HEALTH AND SAFETY CODE - HSC**DIVISION 105. COMMUNICABLE DISEASE PREVENTION AND CONTROL [120100 - 122450] (Division 105 added by Stats. 1995, Ch. 415, Sec. 7.)****PART 4. HUMAN IMMUNODEFICIENCY VIRUS (HIV) [120775 - 121349.3] (Part 4 added by Stats. 1995, Ch. 415, Sec. 7.)****CHAPTER 7. Mandated Blood Testing and Confidentiality to Protect Public Health [120975 - 121023] (Chapter 7 added by Stats. 1995, Ch. 415, Sec. 7.)**
120991.

(a) Each patient who has blood drawn at a primary care clinic and who has consented to the HIV test pursuant to Section 120990 shall be offered an HIV test. The primary care clinician shall offer an HIV test consistent with the United States Preventive Services Task Force recommendation for screening HIV infection. This subdivision shall not apply if the primary care clinic has tested the patient for HIV or if the patient has been offered the HIV test and declined the test within the

previous 12 months. Any subsequent testing of a patient who has been tested by the primary care clinic shall be consistent with the most recent guidelines issued by the United States Preventive Services Task Force.

(b) HIV testing of minors 12 years of age or older shall comply with Section 6926 of the Family Code.

(c) This section shall not prohibit a primary care clinic from charging a patient to cover the cost of HIV testing. The primary care clinic shall be deemed to have complied with this section if an HIV test is offered.

(d) A primary care clinic shall attempt to provide test results to the patient before he or she leaves the facility. If that is not possible, the facility may inform the patient who tests negative for HIV by letter or by telephone, and shall inform a patient with a positive test result in a manner consistent with state law. However, in any case, the primary care clinic shall comply with subdivision (g) of Section 120990.

(e) For purposes of this section, "primary care clinic" means a primary care clinic as defined in subdivision (a) of Section 1204 or subdivision (g), (h), or (j) of Section 1206.

(Added by Stats. 2013, Ch. 589, Sec. 2. Effective January 1, 2014.)

MEDICAL RECORDS COPY FEES

Health & Safety Code §§123100-123149.5

(a) Any patient or his representative is entitled to inspect his medical records during business hours, within five working days after making a written request, subject to payment of reasonable clerical costs. He may bring any one person with him. (HSC 123110(a)) He is entitled to copies of his medical records, to be sent within 15 days of the provider's receipt of a written request, subject to copying costs of not over 25 cents per page plus reasonable clerical costs. ((HSC 123110(b))) The provider may choose to send copies of x-rays and ekgs, eegs, or emgs to another health professional rather than give them to the patient. 15 day limit still applies. ((HSC 123110(c)))

(b) Providers may not withhold records because of unpaid bills. ((HSC 123110(g)))

(c) A health care provider may choose to prepare a summary of the record, for inspection and copying by a patient within 10 working days from the date of the patient's request, rather than allowing access to the entire record. (HSC 123130(a)) However, if more time is needed because the record is of extraordinary length or because the patient was discharged from a facility within the last 10 days, the health care provider shall notify the patient of this fact and deliver the summary within 30 days.

(d) Providers must save records for 7 years or till a minor reaches 19 years old, whichever is longer. (HSC 123145(a))

(e) Patients may submit a 250 word addendum of additions or corrections to the medical record, which must be kept and distributed with the record. ((HSC 123111(a)))

(f) Any individual health care provider who willfully violates this chapter is guilty of unprofessional conduct. (HSC 123110(f))

(g) Any institutional health care provider that willfully violates this chapter is punishable by a fine of not more than \$100. Violation may also be grounds for suspension or revocation of the provider's license or certificate. If the HMO or doctor balks at providing the records, the first step would be to complain to the California Medical Board, (800) 633-2322. In addition the patient may bring an action against the health care provider to enforce these obligations, including, in the discretion of the court, an award of costs and reasonable attorney fees to the prevailing party. (HSC 123120)

RESOURCES

California Legislative Information

- <http://leginfo.legislature.ca.gov>

California Department of Public Health

- <https://www.cdph.ca.gov>

Medical Records Copy Fees

- <http://www.harp.org/og/inforite.htm>

CONTACT INFORMATION

THE MEDICAL BOARD OF CALIFORNIA
2005 EVERGREEN STREET, SUITE 1200
SACRAMENTO, CA 95815
webmaster@mbc.ca.gov
1-800-633-2322