Title 22. Social Security
Division 5. Licensing and Certification of Health Facilities, Home Health Agencies, Clinics, and Referral Agencies
Chapter 13. Medical Information Breach
Article 1. Administrative Penalties

Adopt Chapter 13, Article 1 as follows:

Section 79900. Applicability.

(a) This article applies to the assessment of administrative penalties for a violation of Health and Safety Code section 1280.15 by a clinic, health facility, home health agency, or hospice licensed pursuant to Health and Safety Code section 1204, 1250, 1725 or 1745.

(b) This article applies to violations occurring on or after the effective date of this regulation. In assessing any administrative penalties as provided in this article and under Health and Safety Code section 1280.15, the Department shall consider the compliance history of a health care facility, including compliance history prior to the effective date of this regulation, the extent to which a health care facility detected violations and took preventative action to correct and prevent past violations from recurring, and whether any factors outside a health care facility's control contributed to a breach.

NOTE: Authority cited: Sections 131000, 131050, 131051, 131052 and 131200, Health and Safety Code. Reference: Section 1280.15, Health and Safety Code.

Section 79901. Definitions.

(a) “Access” means the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource.

(b) “Breach” means each individual instance of unlawful or unauthorized access to, use, or disclosure of a specific patient’s medical information.

(1) Breach excludes:

(A) Any paper record, electronic mail, or facsimile transmission inadvertently accessed, used, or disclosed within the same health care facility or health care system where the information is not further accessed, used, or disclosed unless permitted or required by law.

(B) Any internal paper record, electronic mail or facsimile transmission outside the same health care facility or health care system sent to a covered entity (as defined under Part 160.103 of Title 45 of the Code of Federal Regulations, as of June 27, 2014) that has been inadvertently misdirected within the course of coordinating care or delivering services.

(C) A disclosure of medical information in which a health care facility or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such medical information.

(D) Any access to, use, or disclosure of medical information permitted or required by state or federal law.

(E) Any lost or stolen encrypted electronic data containing a patient’s medical information that is in any way created, kept, or maintained by a health care facility where the encrypted electronic data has not been accessed, used, or disclosed in an

unlawful or unauthorized manner. Any lost or stolen electronic data containing a patient's medical information that is in any way created, kept, or maintained by a health care facility that is not encrypted shall be presumed a breach unless it is excluded by section 79901(b)(1)(F).

(F) A disclosure for which a health care facility or business associate, as applicable, determines that there is a low probability that medical information has been compromised based on a risk assessment of at least the following factors:

(i) The nature and extent of the medical information involved, including the types of identifiers and the likelihood of re-identification;

(ii) The unauthorized person who used the medical information or to whom the disclosure was made;

(iii) Whether the medical information was actually acquired or viewed; and

(iv) The extent to which the risk of access to the medical information has been mitigated.

(c) "Business associate" means a person or entity that, in the course of a contractual agreement with a health care facility or health care system:

(1) Creates, receives, maintains, or transmits medical information on behalf of the heath care facility or heath care system for a function or activity regulated by Subchapter C of Subtitle A of Title 45 of the Code of Federal Regulations as of January 25, 2013.

(2) Provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services for which the provision of the services involves the disclosure of medical information to the person or entity.

(3) “Business associate” includes a subcontractor or agent that creates, receives, maintains, or transmits medical information in the course of a contractual agreement with a business associate of a health care facility or health care system.

(4) “Business associate” excludes a workforce member of the health care facility, health care systems affiliated with the health care facility, and providers of health care, as defined under Civil Code section 56.05.

(d) “Business day” means any calendar day except Saturday and Sunday, or the following business holidays: New Year's Day, Martin Luther King Jr. Day, Presidents’ Day, Memorial Day, Independence Day, Labor Day, Veterans' Day, Thanksgiving Day, and Christmas Day.

(e) “Department” means the California Department of Public Health.

(f) “Detect” means the discovery of a breach, or the reasonable belief that a breach occurred by a health care facility or business associate. A breach shall be treated as detected as of the first business day on which such breach is known to the health care facility or business associate, or by exercising reasonable diligence would have been known to the health care facility or business associate. A health care facility or business associate shall be deemed to have knowledge of a breach if such a breach is known, or by exercising reasonable diligence would have been known, to any person other than the person committing the breach, who is a workforce member or agent of the health care facility or a business associate.

(g) “Disclosure” means the release, transfer, provision of access to, or divulging in any manner of information from the entity or individual holding the information.

(h) “Encrypted” means the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key and such confidential process or key that might enable decryption has not been breached.

(i) “Factors outside the control of the health care facility” means any circumstance not within the reasonable control of the health care facility, including, but not limited to, fires, explosions, natural disasters, severe weather events, war, invasion, civil unrest, acts or threats of terrorism, and utility or infrastructure failure. “Factors outside the control of the health care facility” does not include the acts of the health care facility, business associate, or their respective workforce members.

(j) “Health care facility” means a clinic, health facility, home health agency or hospice licensed pursuant to section 1204, 1250, 1725, or 1745 of the Health and Safety Code. For purposes of this chapter, a “health care facility” as it relates to a breach of a patient’s medical information shall include workforce members, medical staff, and business associates at the time of the breach and the detection of the breach.

(k) “Health care system” means:

(1) Health care facilities, along with members of their medical staff and entities under common ownership or control;

(2) Entities participating in an “organized health care arrangement,” as defined under Part 160.103 of Title 45 of the Code of Federal Regulations, as of June 27, 2014;

(3) Entities designated as “affiliated covered entities,” pursuant to Part 164.105(b) of Title 45 of the Code of Federal Regulations, as of March 26, 2013; and

(4) Entities participating in a health care provider network or health plan network, including but not limited to accountable care organizations as defined under Part 425.20 of Title 42 of the Code of Federal Regulations, as of August 9, 2016.

(l) “Medical Information” means, as provided for under Civil Code section 56.05, 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, as defined in Civil Code section 56.05(d), regarding a patient’s medical history, mental or physical condition, or treatment. The term “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.

(m) “Medical staff” shall have the same meaning as provided in section 70703(a)(1).

(n) “Patient representative” shall have the same meaning as provided in Health and Safety Code section 123105(e).

(o) “Reported event” means all breaches included in any single report that is made pursuant to Health and Safety Code section 1280.15(b), regardless of the number of breach events contained in the report.

(p) “Subsequent occurrence” means any additional breach of a patient’s medical information subsequent to a reported event that is substantially related to the initial reported event.

(q) “Unauthorized” shall have the same meaning as provided in Health and Safety Code section 1280.15.

(r) “Workforce” means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a health care facility or business associate, is under the direct control of such health care facility or business associate, whether or not they are paid by the health care facility or business associate.

NOTE: Authority cited: Sections 131000, 131050, 131051, 131052 and 131200, Health and Safety Code. Reference: Section 1280.15, Health and Safety Code.

Section 79902. Breach Reporting Requirements.

(a) A health care facility, excluding a business associate, shall report to the Department a breach of a patient's medical information, or a breach reasonably believed to have occurred, no later than 15 business days after the breach has been detected. Such breaches shall be reported to the Department by the health care facility by electronic mail, telephone, facsimile transmission, first-class mail, or through an internet website maintained by the Department.

(1) In its reporting of a breach, the health care facility shall provide the Department, in writing and signed by a representative of the health care facility, the following:

(A) Name and address of the health care facility where the breach occurred;

(B) Date and time that each breach occurred;

(C) Date and time that each breach was detected;

(D) Name of patient(s) affected;

(E) Description of the medical information that was breached, including the nature and extent of the medical information involved, including the types of individually identifiable information (as defined in Civil Code section 56.05), and the likelihood of re-identification;

(F) Description of the events surrounding the breach;

(G) Name(s) and contact information of the individual(s) who performed the breach, any witness(es) to the breach, and any unauthorized person(s) who used the medical information or to whom the disclosure was made, to the extent known;

(H) Date that patient or patient's representative was notified, was attempted to be notified, or will be notified of breach;

(I) The contact information of a health care facility representative whom the Department may contact for additional information;

(J) Description of any corrective or mitigating action taken by the health care facility;

(K) Any other instances of a reported event that includes a breach of that patient's medical information by the health care facility in the previous six years.

(L) A copy of the notification sent to the patient or patient's representative, pursuant to section 79902(b), and any additional information provided to the patient or patient's representative relating to the breach; and

(M) Any audit reports, witness statements, or other documents that the health care facility relied upon in determining that a breach occurred.

(2) A health care facility shall report any additional information relevant to the breach, as it becomes available to the health care facility, beyond the 15 business days.

(3) If a health care facility fails to report a breach of a patient's medical information to the Department, the Department may assess a penalty in the amount of $100 for each day that the breach is not reported to the Department, not to exceed the limits set forth in Health and Safety Code section 1280.15.

(4) A breach shall not be deemed reported to the Department unless the health care facility has provided, or made a good faith effort to provide, to the Department the items required in section 79902(a)(1). Any items required for reporting under section 79902(a)(1) not available to the health care facility at the time of the reporting shall be

provided to the Department as they are available to the health care facility. Any unreasonable delays in reporting by the health care facility pursuant to this subdivision are subject to an administrative penalty assessed pursuant to section 79902(a)(3). In assessing whether delay is unreasonable, the Department will consider, among other factors, the size of the affected population, lack of sufficient information in the reporting of an incident to make a determination of compliance, time passed between the time of an incident and its discovery, whether the cause of an incident was a business associate or workforce member, and availability of staff to respond to an incident.

(5) In the event a health care facility has performed, pursuant to section 79901(b)(1)(F), a risk assessment and has determined that an incident does not constitute a breach of a patient's medical information, the health care facility shall maintain a centralized record of each non-breach incident, along with all materials the health care facility relied upon in performing the risk assessment. All such centralized records shall be maintained by the health care facility and available for inspection by the Department at all times. A health care facility shall retain records relating to such a risk assessment for a period of at least six years from the time of the incident.

(b) Except as provided in Health and Safety Code section 1280.15(c), a health care facility shall report a breach of a patient's medical information in writing by first-class mail to the patient or the patient's representative at the last known address, or by electronic mail, if the individual agrees and such agreement has not been withdrawn, pursuant to Part 164.404(d) of Title 45 of the Code of Federal Regulations, no later than 15 business days after the breach has been detected by the health care facility. The notification may be provided in one or more mailings as information is available.

(1) In its reporting of the breach, the health care facility shall provide the patient or the patient's representative:

(A) A brief description of what happened, including the health care facility name and address, the date of the breach and the date of the discovery of the breach, if known;

(B) A description of the types of medical information that were involved in the breach (e.g., full name, Social Security number, date of birth, home address, account number, diagnosis, or other types of information);

(C) Any steps the patient should take to protect himself or herself from potential harm resulting from the breach;

(D) A brief description of what the health care facility involved is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and

(E) Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, internet website address, or postal address.

(2) The reporting required in subsection (b)(1) shall be written in plain language.

(3) If a health care facility does not report a breach of a patient's medical information to a patient or the patient's representative, the Department may assess a penalty in the amount of $100 for each day that the breach is not reported to the patient or the patient's representative, not to exceed the limits set forth in Health and Safety Code section 1280.15.

NOTE: Authority cited: Sections 131000, 131050, 131051, 131052 and 131200, Health and Safety Code. Reference: Section 1280.15, Health and Safety Code.

Section 79903. Administrative Penalties.

(a) The Department may impose an administrative penalty upon a health care facility if the Department determines that the health care facility has committed a breach of a patient's medical information. The penalty assessed for any violation in accordance with this article, including penalty adjustment factors, shall not exceed the maximum penalty specified in Health and Safety Code section 1280.15.

(b) When the Department has determined that an administrative penalty for a breach of a patient's medical information is warranted, the base penalty amount is $15,000 for each violation, subject to the penalty adjustment factors provided in section 79904.

(c) For each subsequent occurrence of a breach of a patient's medical information relating to a particular reported event, the Department may assess an administrative penalty in an amount equal to 70% of the initial violation's final penalty amount. The administrative penalty for the subsequent occurrence shall be subject to the penalty adjustment factors pursuant to section 79904, if applicable, not to exceed the statutory maximum of $17,500 per subsequent occurrence.

NOTE: Authority cited: Sections 131000, 131050, 131051, 131052 and 131200, Health and Safety Code. Reference: Section 1280.15, Health and Safety Code.

Section 79904. Penalty Adjustment Factors.

(a) Using the following factors, the base penalty assessed pursuant to sections 79903(b) and (c) shall be increased or decreased by up to $10,000 to calculate the final penalty:

(1) The health care facility's history of compliance with Health and Safety Code section 1280.15 and other related state and federal law for the past three calendar years.

(2) The extent to which the health care facility detected violations and took preventative action to immediately correct and prevent past violations from recurring.

(3) Factors outside the control of the health care facility as defined by section 79901(i). There shall be no penalty if the health care facility developed and maintained disaster and emergency policies and procedures that were appropriately implemented during a disaster or emergency, if factors outside the control of the health care facility as referenced in 79901(i) were the sole cause of a breach.

(4) Any other factors applicable to the specific circumstances surrounding the breach, as identified by the Department.

(b) The Department may reduce a final penalty amount as calculated pursuant to section 79904 if the Department determines that the administrative penalty is unduly burdensome or excessive.

NOTE: Authority cited: Sections 131000, 131050, 131051, 131052 and 131200, Health and Safety Code. Reference: Section 1280.15, Health and Safety Code.

Section 79905. Small and Rural Hospitals; Primary Care Clinics; and Skilled Nursing Facilities.

(a) In assessing an administrative penalty for a breach of a patient's medical information pursuant to Health and Safety Code section 1280.15 by a health care facility that is a small and rural hospital, as defined by Health and Safety Code section 124840, or its business associates, the Department may modify the penalty upon timely request from the small and rural hospital.

(1) The small and rural hospital that has been assessed an administrative penalty may request:

(A) Payment of the administrative penalty extended over a period of time if immediate, full payment would cause financial hardship;

(B) Reduction of the penalty if extending the penalty payment over a period of time would cause financial hardship; or

(C) Both penalty payment extension and reduction of the penalty.

(2) The small and rural hospital shall submit its written request for penalty modification to the Department within 10 calendar days after the issuance of an administrative penalty. The request shall describe the specific circumstances showing financial hardship to the hospital and the potential adverse effects on access to quality care in the hospital.

(b) In assessing an administrative penalty for a breach of a patient's medical information pursuant to Health and Safety Code section 1280.15 by a health care facility that is a primary care clinic, as defined by Health and Safety Code section 1204(a), or its business associates, the Department shall reduce the base penalty as provided for in

section 79903(b) by one half. The Department shall subsequently determine the final penalty by considering penalty adjustment factors under section 79904 reduced by one half.

(c) When assessing penalties on a skilled nursing facility or other health care facility subject to Health and Safety Code section 1423, 1424, 1424.1, or 1424.5 and under this Article, the Department shall only issue the higher of either a penalty under this Article or a penalty for a violation of section 1423, 1424, 1424.1, or 1424.5, but not both.

NOTE: Authority cited: Sections 131000, 131050, 131051, 131052 and 131200, Health and Safety Code. Reference: Section 1280.15, Health and Safety Code.