AMENDED IN ASSEMBLY MARCH 28, 2014

CALIFORNIA LEGISLATURE—2013–14 REGULAR SESSION

ASSEMBLY BILL No. 1755

Introduced by Assembly Member Gomez

February 14, 2014

An act to amend Section 1280.15 of the Health and Safety Code, relating to public health.

LEGISLATIVE COUNSEL'S DIGEST

AB 1755, as amended, Gomez. Medical information.

Existing law requires a clinic, health facility, home health agency, or hospice to prevent unlawful or unauthorized access to, and use or disclosure of, patients' medical information, as defined. Existing law requires the clinic, health facility, home health agency, or hospice to report any unlawful or unauthorized access to, or use or disclosure of, a patient's medical information to the State Department of Public Health and to the affected patient or the patient's representative~~, as prescribed~~ *no later than 5 business days after the unlawful or unauthorized access, use, or disclosure has been detected*. Existing law authorizes the State Department of Public Health to assess administrative penalties for violation of these provisions.

~~This bill would make technical, nonsubstantive changes to these provisions.~~

This bill would instead require those entities to prevent breaches of patients' medical information, as defined, and to report any breach of a patient's medical information to the department and to the affected patient or the patient's representative without unreasonable delay and in no case later than 60 calendar days after the breach has been detected, as specified.

Vote: majority. Appropriation: no. Fiscal committee: no. State-mandated local program: no.

The people of the State of California do enact as follows:

SECTION 1. Section 1280.15 of the Health and Safety Code is amended to read:

1280.15. (a) A clinic, health facility, home health agency, or hospice licensed pursuant to Section 1204, 1250, 1725, or 1747 shall prevent ~~unlawful or unauthorized access to, and use or disclosure of,~~ *breaches of* patients' medical information~~, as defined in Section 56.05 of the Civil Code and consistent with~~ *as required by* Section 130203. For purposes of this section, internal paper records, ~~electronic mail,~~ *e-mail*, or facsimile transmissions inadvertently misdirected within the same facility or health care system within the course of coordinating care or delivering services shall not constitute ~~unauthorized access to, or use or disclosure of,~~ *a breach of* a patient's medical information. The department, after investigation, may assess an administrative penalty for a violation of this section of up to twenty-five thousand dollars ($25,000) per patient whose medical information was ~~unlawfully or without authorization accessed, used, or disclosed,~~ *breached*, and up to seventeen thousand five hundred dollars ($17,500) per subsequent ~~occurrence of unlawful or unauthorized access, use, or disclosure of~~ *breach of* that patient's medical information. For purposes of the investigation, the department shall consider the clinic's, health facility's, agency's, or hospice's history of compliance with this section and other related state and federal statutes and regulations, the extent to which the facility detected violations and took preventative action to immediately correct and prevent past violations from recurring, and factors outside its control that restricted the facility's ability to comply with this section. The department shall have full discretion to consider all factors when determining the amount of an administrative penalty pursuant to this section.

(b) (1) A clinic, health facility, home health agency, or hospice to which subdivision (a) applies shall report any ~~unlawful or unauthorized access to, or use or disclosure of,~~ *breach of* a patient's medical information to the department ~~no later than five business days after the unlawful or unauthorized access, use, or disclosure~~

without unreasonable delay and in no case later than 60 calendar days after the breach has been detected by the clinic, health facility, home health agency, or hospice.

(2) Subject to subdivision (c), a clinic, health facility, home health agency, or hospice shall also report any ~~unlawful or unauthorized access to, or use or disclosure of,~~ *breach of* a patient's medical information to the affected patient or the patient's representative at the last known address, ~~no later than five business days after the unlawful or unauthorized access, use, or disclosure~~, *or by an alternative means or at an alternative location as specified by the patient or the patient's representative in writing pursuant to Section 164.522(b) of Title 45 of the Code of Federal Regulations, without unreasonable delay and in no case later than 60 calendar days after the breach* has been detected by the clinic, health facility, home health agency, or hospice. *Notice may be provided by e-mail only if the patient has previously agreed in writing to electronic notice by e-mail.*

(c) (1) A clinic, health facility, home health agency, or hospice shall delay the reporting, as required pursuant to paragraph (2) of subdivision (b), of any ~~unlawful or unauthorized access to, or use or disclosure of,~~ *breach of* a patient's medical information ~~beyond five business days~~ if a law enforcement agency or official provides the clinic, health facility, home health agency, or hospice with a written or oral statement that compliance with the reporting requirements of paragraph (2) of subdivision (b) would likely impede the law enforcement agency's investigation that relates to the ~~unlawful or unauthorized access to, and use or disclosure of,~~ *breach of* a patient's medical information and specifies a date upon which the delay shall end, not to exceed 60 days after a written request is made, or 30 days after an oral request is made. A law enforcement agency or official may request an extension of a delay based upon a written declaration that there exists a bona fide, ongoing, significant criminal investigation of serious wrongdoing relating to the ~~unlawful or unauthorized access to, and use or disclosure of,~~ *breach of* a patient's medical information, that notification of patients will undermine the law enforcement agency's investigation, and that specifies a date upon which the delay shall end, not to exceed 60 days after the end of the original delay period.

(2) If the statement of the law enforcement agency or official is made orally, then the clinic, health facility, home health agency, or hospice shall do both of the following:

(A) Document the oral statement, including, but not limited to, the identity of the law enforcement agency or official making the oral statement and the date upon which the oral statement was made.

(B) Limit the delay in reporting the ~~unlawful or unauthorized access to, or use or disclosure of,~~ *breach of* the patient's medical information to the date specified in the oral statement, not to exceed 30 calendar days from the date that the oral statement is made, unless a written statement that complies with the requirements of this subdivision is received during that time.

(3) A clinic, health facility, home health agency, or hospice shall submit a report that is delayed pursuant to this subdivision not later than five business days after the date designated as the end of the delay.

(d) If a clinic, health facility, home health agency, or hospice to which subdivision (a) applies violates subdivision (b), the department may assess the licensee a penalty in the amount of one hundred dollars ($100) for each day that the ~~unlawful or unauthorized access, use, or disclosure~~ *breach* is not reported to the department or the affected patient, following the initial ~~five-day~~ period specified in subdivision (b). However, the total combined penalty assessed by the department under subdivision (a) and this subdivision shall not exceed two hundred fifty thousand dollars ($250,000) per reported event. For enforcement purposes, it shall be presumed that the facility did not notify the affected patient if the notification was not documented. This presumption may be rebutted by a licensee only if the licensee demonstrates, by a preponderance of the evidence, that the notification was made.

(e) In enforcing subdivisions (a) and (d), the department shall take into consideration the special circumstances of small and rural hospitals, as defined in Section 124840, and primary care clinics, as defined in subdivision (a) of Section 1204, in order to protect access to quality care in those hospitals and clinics. When assessing a penalty on a skilled nursing facility or other facility subject to Section 1423, 1424, 1424.1, or 1424.5, the department shall issue only the higher of either a penalty for the violation of this section

or a penalty for violation of Section 1423, 1424, 1424.1, or 1424.5, not both.

(f) All penalties collected by the department pursuant to this section and Sections 1280.1, 1280.3, and 1280.4 shall be deposited into the Internal Departmental Quality Improvement Account, which is hereby created within the Special Deposit Fund under Section 16370 of the Government Code. Upon appropriation by the Legislature, moneys in the account shall be expended for internal quality improvement activities in the Licensing and Certification Program.

(g) If the licensee disputes a determination by the department regarding a failure to prevent or failure to timely report ~~unlawful or unauthorized access to, or use or disclosure of,~~ *a breach of* patients' medical information, or the imposition of a penalty under this section, the licensee may, within 10 days of receipt of the penalty assessment, request a hearing pursuant to Section 131071. Penalties shall be paid when appeals have been exhausted and the penalty has been upheld.

(h) In lieu of disputing the determination of the department regarding a failure to prevent or failure to timely report ~~unlawful or unauthorized access to, or use or disclosure of,~~ *a breach of* patients' medical information, transmit to the department 75 percent of the total amount of the administrative penalty, for each violation, within 30 business days of receipt of the administrative penalty.

(i) Notwithstanding any other law, the department may refer violations of this section to the Office of Health Information Integrity for enforcement pursuant to Section 130303.

(j) For purposes of this section, the following definitions shall apply:

(1) "Breach" means the acquisition, access, use, or disclosure of unsecured medical information in a manner not permitted under state or federal health information privacy laws that compromises the security or privacy of the medical information.

(A) "Breach" does not include any of the following:

(i) Any unintentional acquisition, access, or use of medical information by a workforce member or person acting under the authority of a clinic, health facility, home health agency, or hospice to which subdivision (a) applies, or a business associate, if that acquisition, access, or use was made in good faith and within the

scope of authority and does not result in further use or disclosure in a manner not permitted under state or federal health information privacy laws.

(ii) Any inadvertent disclosure by a person who is authorized to access medical information at a clinic, health facility, home health agency, or hospice to which subdivision (a) applies or a business associate to another person authorized to access medical information at the same entity or business associate, or organized health care arrangement in which the clinic, health facility, home health agency, or hospice to which subdivision (a) participates, and the information received as a result of the disclosure is not further used or disclosed in a manner not permitted under state or federal health information privacy laws.

(iii) A disclosure of medical information when a clinic, health facility, home health agency, or hospice to which subdivision (a) applies 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 the information.

(B) Except as provided in subdivision (a) and subparagraph (A), an acquisition, access, use, or disclosure of medical information in a manner not permitted under state or federal health information privacy laws is presumed to be a breach unless the clinic, health facility, home health agency, or hospice to which subdivision (a) applies or business associate, as applicable, demonstrates that there is a low probability that the 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 reidentification.

(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.

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

(2) "Business associate" has the meaning provided in regulations issued pursuant to the Health Information Portability and Accountability Act of 1996 (Public Law 104-191)(HIPAA)

found in Parts 160 and 164 of Title 45 of the Code of Federal Regulations.

(3) "Detected" means that sufficient facts are known about an incident such that a reasonable person would believe that a breach of a patient's medical information has taken place.

(4) "Medical information" has the meaning provided in Section 56.05 of the Civil Code.

(5) "Organized health care arrangement" has the meaning provided in regulations issued pursuant to HIPAA found in Parts 160 and 164 of Title 45 of the Code of Federal Regulations.

~~(1)~~

(6) "Reported event" means all breaches included in any single report that is made pursuant to subdivision (b), regardless of the number of breach events contained in the report.

~~(2)~~

(7) "Unauthorized" means the inappropriate access, review, or viewing of patient medical information without a direct need for medical diagnosis, treatment, or other lawful use as permitted by the Confidentiality of Medical Information Act (Part 2.6 (commencing with Section 56) of Division 1 of the Civil Code) or any other statute or regulation governing the lawful access, use, or disclosure of medical information.

(8) "Unsecured medical information" means medical information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons though use of a technology or methodology specified by the United States Secretary of Health and Human Services in the guidance issued under Section 13402(h)(2) of the American Recovery and Reinvestment Act of 2009 (Public Law 111-5).

(9) "Workforce" has the meaning provided in regulations issued pursuant to HIPAA found in Parts 160 and 164 of Title 45 of the Code of Federal Regulations.

O