

AMENDED IN SENATE JULY 1, 2014
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 no later than 5 business days after the unlawful or unauthorized access, use, or disclosure has been detected. *Existing law requires that the report to the patient or the patient's representative be made to that person's last known address. Existing law requires these entities to delay the report for specified law enforcement purposes and requires that the delayed report be submitted within 5 days of the end of the delay.* Existing law authorizes the State Department of Public Health to assess administrative penalties for violation of these provisions *and gives the department discretion to consider all factors when determining the amount of a penalty.*

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 *to make those reports no later than 15 business days after the breach unlawful or unauthorized access, use, or disclosure has been detected, as specified and would authorize the report made to the patient or the patient’s representative to be made by alternative means, including email, as specified. The bill would also require a delayed report for law enforcement purposes to be made within 15 business days of the end of the delay. The bill would give the department full discretion to consider all factors when determining whether to investigate under these provisions.*

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

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

1 SECTION 1. Section 1280.15 of the Health and Safety Code
 2 is amended to read:
 3 1280.15. (a) A clinic, health facility, home health agency, or
 4 hospice licensed pursuant to Section 1204, 1250, 1725, or 1745
 5 shall prevent unlawful or unauthorized access to, and use or
 6 disclosure of, patients’ medical information, as defined in Section
 7 56.05 of the Civil Code and consistent with Section 130203. For
 8 purposes of this section, internal paper records, electronic mail,
 9 or facsimile transmissions inadvertently misdirected within the
 10 same facility or health care system within the course of
 11 coordinating care or delivering services shall not constitute
 12 unauthorized access to, or use or disclosure of, a patient’s medical
 13 information. The department, after investigation, may assess an
 14 administrative penalty for a violation of this section of up to
 15 twenty-five thousand dollars (\$25,000) per patient whose medical
 16 information was unlawfully or without authorization accessed,
 17 used, or disclosed, and up to seventeen thousand five hundred
 18 dollars (\$17,500) per subsequent occurrence of unlawful or
 19 unauthorized access, use, or disclosure of that patient’s medical
 20 information. For purposes of the investigation, the department
 21 shall consider the clinic’s, health facility’s, agency’s, or hospice’s
 22 history of compliance with this section and other related state and

1 federal statutes and regulations, the extent to which the facility
2 detected violations and took preventative action to immediately
3 correct and prevent past violations from recurring, and factors
4 outside its control that restricted the facility's ability to comply
5 with this section. The department shall have full discretion to
6 consider all factors when determining *whether to investigate and*
7 *the amount of an administrative penalty, if any,* pursuant to this
8 section.

9 (b) (1) A clinic, health facility, home health agency, or hospice
10 to which subdivision (a) applies shall report any unlawful or
11 unauthorized access to, or use or disclosure of, a patient's medical
12 information to the department no later than ~~five~~ 15 business days
13 after the unlawful or unauthorized access, use, or disclosure has
14 been detected by the clinic, health facility, home health agency,
15 or hospice.

16 (2) Subject to subdivision (c), a clinic, health facility, home
17 health agency, or hospice shall also report any unlawful or
18 unauthorized access to, or use or disclosure of, a patient's medical
19 information to the affected patient or the patient's representative
20 at the last known address, *or by an alternative means or at an*
21 *alternative location as specified by the patient or the patient's*
22 *representative in writing pursuant to Section 164.522(b) of Title*
23 *45 of the Code of Federal Regulations,* no later than ~~five~~ 15
24 business days after the unlawful or unauthorized access, use, or
25 disclosure has been detected by the clinic, health facility, home
26 health agency, or hospice. *Notice may be provided by email only*
27 *if the patient has previously agreed in writing to electronic notice*
28 *by email.*

29 (c) (1) A clinic, health facility, home health agency, or hospice
30 shall delay the reporting, as required pursuant to paragraph (2) of
31 subdivision (b), of any unlawful or unauthorized access to, or use
32 or disclosure of, a patient's medical information beyond ~~five~~ 15
33 business days if a law enforcement agency or official provides the
34 clinic, health facility, home health agency, or hospice with a written
35 or oral statement that compliance with the reporting requirements
36 of paragraph (2) of subdivision (b) would likely impede the law
37 enforcement agency's investigation that relates to the unlawful or
38 unauthorized access to, and use or disclosure of, a patient's medical
39 information and specifies a date upon which the delay shall end,
40 not to exceed 60 days after a written request is made, or 30 days

1 after an oral request is made. A law enforcement agency or official
2 may request an extension of a delay based upon a written
3 declaration that there exists a bona fide, ongoing, significant
4 criminal investigation of serious wrongdoing relating to the
5 unlawful or unauthorized access to, and use or disclosure of, a
6 patient's medical information, that notification of patients will
7 undermine the law enforcement agency's investigation, and that
8 specifies a date upon which the delay shall end, not to exceed 60
9 days after the end of the original delay period.

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

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

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

23 (3) A clinic, health facility, home health agency, or hospice
24 shall submit a report that is delayed pursuant to this subdivision
25 not later than ~~five~~ 15 business days after the date designated as the
26 end of the delay.

27 (d) If a clinic, health facility, home health agency, or hospice
28 to which subdivision (a) applies violates subdivision (b), the
29 department may assess the licensee a penalty in the amount of one
30 hundred dollars (\$100) for each day that the unlawful or
31 unauthorized access, use, or disclosure is not reported to the
32 department or the affected patient, following the initial ~~five-day~~
33 15-day period specified in subdivision (b). However, the total
34 combined penalty assessed by the department under subdivision
35 (a) and this subdivision shall not exceed two hundred fifty thousand
36 dollars (\$250,000) per reported event. For enforcement purposes,
37 it shall be presumed that the facility did not notify the affected
38 patient if the notification was not documented. This presumption
39 may be rebutted by a licensee only if the licensee demonstrates,
40 by a preponderance of the evidence, that the notification was made.

1 (e) In enforcing subdivisions (a) and (d), the department shall
2 take into consideration the special circumstances of small and rural
3 hospitals, as defined in Section 124840, and primary care clinics,
4 as defined in subdivision (a) of Section 1204, in order to protect
5 access to quality care in those hospitals and clinics. When assessing
6 a penalty on a skilled nursing facility or other facility subject to
7 Section 1423, 1424, 1424.1, or 1424.5, the department shall issue
8 only the higher of either a penalty for the violation of this section
9 or a penalty for violation of Section 1423, 1424, 1424.1, or 1424.5,
10 not both.

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

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

27 (h) In lieu of disputing the determination of the department
28 regarding a failure to prevent or failure to timely report unlawful
29 or unauthorized access to, or use or disclosure of, patients' medical
30 information, transmit to the department 75 percent of the total
31 amount of the administrative penalty, for each violation, within
32 30 business days of receipt of the administrative penalty.

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

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

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

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

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

10 ~~1280.15. (a) A clinic, health facility, home health agency, or~~
11 ~~hospice licensed pursuant to Section 1204, 1250, 1725, or 1747~~
12 ~~shall prevent breaches of patients’ medical information as required~~
13 ~~by Section 130203. For purposes of this section, internal paper~~
14 ~~records, e-mail, or facsimile transmissions inadvertently~~
15 ~~misdirected within the same facility or health care system within~~
16 ~~the course of coordinating care or delivering services shall not~~
17 ~~constitute a breach of a patient’s medical information. The~~
18 ~~department, after investigation, may assess an administrative~~
19 ~~penalty for a violation of this section of up to twenty-five thousand~~
20 ~~dollars (\$25,000) per patient whose medical information was~~
21 ~~breached, and up to seventeen thousand five hundred dollars~~
22 ~~(\$17,500) per subsequent breach of that patient’s medical~~
23 ~~information. For purposes of the investigation, the department~~
24 ~~shall consider the clinic’s, health facility’s, agency’s, or hospice’s~~
25 ~~history of compliance with this section and other related state and~~
26 ~~federal statutes and regulations, the extent to which the facility~~
27 ~~detected violations and took preventative action to immediately~~
28 ~~correct and prevent past violations from recurring, and factors~~
29 ~~outside its control that restricted the facility’s ability to comply~~
30 ~~with this section. The department shall have full discretion to~~
31 ~~consider all factors when determining the amount of an~~
32 ~~administrative penalty pursuant to this section.~~

33 ~~(b) (1) A clinic, health facility, home health agency, or hospice~~
34 ~~to which subdivision (a) applies shall report any breach of a~~
35 ~~patient’s medical information to the department without~~
36 ~~unreasonable delay and in no case later than 60 calendar days after~~
37 ~~the breach has been detected by the clinic, health facility, home~~
38 ~~health agency, or hospice.~~

39 ~~(2) Subject to subdivision (c), a clinic, health facility, home~~
40 ~~health agency, or hospice shall also report any breach of a patient’s~~

1 ~~medical information to the affected patient or the patient's~~
2 ~~representative at the last known address,, or by an alternative means~~
3 ~~or at an alternative location as specified by the patient or the~~
4 ~~patient's representative in writing pursuant to Section 164.522(b)~~
5 ~~of Title 45 of the Code of Federal Regulations, without~~
6 ~~unreasonable delay and in no case later than 60 calendar days after~~
7 ~~the breach has been detected by the clinic, health facility, home~~
8 ~~health agency, or hospice. Notice may be provided by e-mail only~~
9 ~~if the patient has previously agreed in writing to electronic notice~~
10 ~~by e-mail.~~

11 ~~(e) (1) A clinic, health facility, home health agency, or hospice~~
12 ~~shall delay the reporting, as required pursuant to paragraph (2) of~~
13 ~~subdivision (b), of any breach of a patient's medical information~~
14 ~~if a law enforcement agency or official provides the clinic, health~~
15 ~~facility, home health agency, or hospice with a written or oral~~
16 ~~statement that compliance with the reporting requirements of~~
17 ~~paragraph (2) of subdivision (b) would likely impede the law~~
18 ~~enforcement agency's investigation that relates to the breach of a~~
19 ~~patient's medical information and specifies a date upon which the~~
20 ~~delay shall end, not to exceed 60 days after a written request is~~
21 ~~made, or 30 days after an oral request is made. A law enforcement~~
22 ~~agency or official may request an extension of a delay based upon~~
23 ~~a written declaration that there exists a bona fide, ongoing,~~
24 ~~significant criminal investigation of serious wrongdoing relating~~
25 ~~to the breach of a patient's medical information, that notification~~
26 ~~of patients will undermine the law enforcement agency's~~
27 ~~investigation, and that specifies a date upon which the delay shall~~
28 ~~end, not to exceed 60 days after the end of the original delay period.~~

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

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

36 ~~(B) Limit the delay in reporting the breach of the patient's~~
37 ~~medical information to the date specified in the oral statement, not~~
38 ~~to exceed 30 calendar days from the date that the oral statement~~
39 ~~is made, unless a written statement that complies with the~~
40 ~~requirements of this subdivision is received during that time.~~

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

5 ~~(d) If a clinic, health facility, home health agency, or hospice~~
6 ~~to which subdivision (a) applies violates subdivision (b), the~~
7 ~~department may assess the licensee a penalty in the amount of one~~
8 ~~hundred dollars (\$100) for each day that the breach is not reported~~
9 ~~to the department or the affected patient, following the initial period~~
10 ~~specified in subdivision (b). However, the total combined penalty~~
11 ~~assessed by the department under subdivision (a) and this~~
12 ~~subdivision shall not exceed two hundred fifty thousand dollars~~
13 ~~(\$250,000) per reported event. For enforcement purposes, it shall~~
14 ~~be presumed that the facility did not notify the affected patient if~~
15 ~~the notification was not documented. This presumption may be~~
16 ~~rebutted by a licensee only if the licensee demonstrates, by a~~
17 ~~preponderance of the evidence, that the notification was made.~~

18 ~~(e) In enforcing subdivisions (a) and (d), the department shall~~
19 ~~take into consideration the special circumstances of small and rural~~
20 ~~hospitals, as defined in Section 124840, and primary care clinics,~~
21 ~~as defined in subdivision (a) of Section 1204, in order to protect~~
22 ~~access to quality care in those hospitals and clinics. When assessing~~
23 ~~a penalty on a skilled nursing facility or other facility subject to~~
24 ~~Section 1423, 1424, 1424.1, or 1424.5, the department shall issue~~
25 ~~only the higher of either a penalty for the violation of this section~~
26 ~~or a penalty for violation of Section 1423, 1424, 1424.1, or 1424.5,~~
27 ~~not both.~~

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

36 ~~(g) If the licensee disputes a determination by the department~~
37 ~~regarding a failure to prevent or failure to timely report a breach~~
38 ~~of patients' medical information, or the imposition of a penalty~~
39 ~~under this section, the licensee may, within 10 days of receipt of~~
40 ~~the penalty assessment, request a hearing pursuant to Section~~

1 ~~131071. Penalties shall be paid when appeals have been exhausted~~
2 ~~and the penalty has been upheld.~~

3 ~~(h) In lieu of disputing the determination of the department~~
4 ~~regarding a failure to prevent or failure to timely report a breach~~
5 ~~of patients' medical information, transmit to the department 75~~
6 ~~percent of the total amount of the administrative penalty, for each~~
7 ~~violation, within 30 business days of receipt of the administrative~~
8 ~~penalty.~~

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

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

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

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

19 ~~(i) Any unintentional acquisition, access, or use of medical~~
20 ~~information by a workforce member or person acting under the~~
21 ~~authority of a clinic, health facility, home health agency, or hospice~~
22 ~~to which subdivision (a) applies, or a business associate, if that~~
23 ~~acquisition, access, or use was made in good faith and within the~~
24 ~~scope of authority and does not result in further use or disclosure~~
25 ~~in a manner not permitted under state or federal health information~~
26 ~~privacy laws.~~

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

37 ~~(iii) A disclosure of medical information when a clinic, health~~
38 ~~facility, home health agency, or hospice to which subdivision (a)~~
39 ~~applies or business associate has a good faith belief that an~~

1 unauthorized person to whom the disclosure was made would not
2 reasonably have been able to retain the information.

3 (B) Except as provided in subdivision (a) and subparagraph (A),
4 an acquisition, access, use, or disclosure of medical information
5 in a manner not permitted under state or federal health information
6 privacy laws is presumed to be a breach unless the clinic, health
7 facility, home health agency, or hospice to which subdivision (a)
8 applies or business associate, as applicable, demonstrates that there
9 is a low probability that the medical information has been
10 compromised based on a risk assessment of at least the following
11 factors:

12 (i) The nature and extent of the medical information involved,
13 including the types of identifiers and the likelihood of
14 reidentification.

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

17 (iii) Whether the medical information was actually acquired or
18 viewed.

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

21 (2) “Business associate” has the meaning provided in regulations
22 issued pursuant to the Health Information Portability and
23 Accountability Act of 1996 (Public Law 104-191)(HIPAA) found
24 in Parts 160 and 164 of Title 45 of the Code of Federal Regulations.

25 (3) “Detected” means that sufficient facts are known about an
26 incident such that a reasonable person would believe that a breach
27 of a patient’s medical information has taken place.

28 (4) “Medical information” has the meaning provided in Section
29 56.05 of the Civil Code.

30 (5) “Organized health care arrangement” has the meaning
31 provided in regulations issued pursuant to HIPAA found in Parts
32 160 and 164 of Title 45 of the Code of Federal Regulations.

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

36 (7) “Unauthorized” means the inappropriate access, review, or
37 viewing of patient medical information without a direct need for
38 medical diagnosis, treatment, or other lawful use as permitted by
39 the Confidentiality of Medical Information Act (Part 2.6
40 (commencing with Section 56) of Division 1 of the Civil Code)

1 or any other statute or regulation governing the lawful access, use,
2 or disclosure of medical information.

3 (8) ~~“Unsecured medical information” means medical information~~
4 ~~that is not rendered unusable, unreadable, or indecipherable to~~
5 ~~unauthorized persons through use of a technology or methodology~~
6 ~~specified by the United States Secretary of Health and Human~~
7 ~~Services in the guidance issued under Section 13402(h)(2) of the~~
8 ~~American Recovery and Reinvestment Act of 2009 (Public Law~~
9 ~~111-5).~~

10 (9) ~~“Workforce” has the meaning provided in regulations issued~~
11 ~~pursuant to HIPAA found in Parts 160 and 164 of Title 45 of the~~
12 ~~Code of Federal Regulations.~~