

AMENDED IN ASSEMBLY MARCH 28, 2016

CALIFORNIA LEGISLATURE—2015–16 REGULAR SESSION

**ASSEMBLY BILL**

**No. 2688**

---

---

**Introduced by Assembly Member Gordon**

February 19, 2016

---

---

An act to ~~amend Section 56.05 of the Civil Code, relating to privacy.~~ *add Chapter 22.4 (commencing with Section 22596) to Division 8 of the Business and Professions Code, relating to privacy.*

LEGISLATIVE COUNSEL'S DIGEST

AB 2688, as amended, Gordon. ~~Medical information privacy: commercial health monitoring device.~~ *Privacy: commercial health monitoring programs.*

Existing federal law, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), establishes certain requirements relating to the provision of health insurance, including provisions relating to the confidentiality of health records. HIPAA prohibits a covered entity that uses electronic means to perform HIPAA-covered transactions, from using or disclosing personal health information except pursuant to a written authorization signed by the patient or for treatment, payment, or health care operations. Notwithstanding those provisions, HIPAA allows a covered entity to maintain a directory of patients in its facility for specified purposes, and to disclose the protected health information of a patient to family members, relatives, or other persons identified by the patient, if certain conditions are met. Covered entities include health plans, health care clearinghouses, such as billing services and community health information systems, and health care providers that transmit health care data in a way that is regulated by HIPAA. HIPAA further provides that if its provisions conflict with a provision

of state law, the provision that is most protective of patient privacy prevails.

Existing law, the Confidentiality of Medical Information Act, prohibits a provider of health care, a health care service plan, a contractor, a corporation and its subsidiaries and affiliates, or any business that offers software or hardware to consumers, including a mobile application or other related device, as defined, from intentionally sharing, selling, using for marketing, or otherwise using any medical information, as defined, for any purpose not necessary to provide health care services to a patient, except as expressly authorized by the patient, enrollee, or subscriber, as specified, or as otherwise required or authorized by law. ~~A violation of the provisions of this act that results in economic loss or personal injury to a patient is a crime.~~

~~The bill would include in the definition of “medical information” for these purposes any individually identifiable information in possession of or derived from a consumer health monitoring device, as defined.~~

~~By expanding the definition of an existing crime, this bill would impose a state-mandated local program by creating new crimes.~~

~~The California Constitution requires the state to reimburse local agencies and school districts for certain costs mandated by the state. Statutory provisions establish procedures for making that reimbursement.~~

~~This bill would provide that no reimbursement is required by this act for a specified reason.~~

*This bill would prohibit an operator of a commercial health monitoring program from intentionally sharing, selling, disclosing, using for marketing, or otherwise using health information in possession of or derived from a commercial health monitoring program to a 3rd party, as defined, without first obtaining explicit authorization, as provided, and would extend this prohibition to a 3rd party that solely provides a service to the program. The bill would also require an employer that receives health information in possession of or derived from a commercial health monitoring program to establish procedures to ensure the confidentiality of, and protection from unauthorized use and disclosure of, that information, as provided. The bill would further prohibit an employer from discriminating against an employee based on an employee’s health information or if that employee does not authorize the use of his or her health information.*

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

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

1     *SECTION 1. Chapter 22.4 (commencing with Section 22596)*  
2 *is added to Division 8 of the Business and Professions Code, to*  
3 *read:*

4  
5     *CHAPTER 22.4. DIGITAL COMMERCIAL HEALTH MONITORING*  
6                                    *PROGRAMS*

7  
8     22596. For purposes of this chapter:

9     (a) “Commercial health monitoring program” means a  
10 *commercial Internet Web site or online service used by consumers*  
11 *that collects health information regarding an individual’s mental*  
12 *or physical condition from sources including, but not limited to,*  
13 *manual entry, sensors, or both.*

14     (b) “Health information” mean any individually identifiable  
15 *information, in electronic or physical form, in possession of, or*  
16 *derived from, a commercial health monitoring program regarding*  
17 *a consumer’s mental or physical condition.*

18     (c) “Individually identifiable” means that the health information  
19 *includes or contains an element of personal identifying information*  
20 *sufficient to allow identification of the individual, including, but*  
21 *not limited to, the individual’s name, address, electronic mail*  
22 *address, telephone number, social security number, or unique*  
23 *electronic identifier, or other information that, alone or in*  
24 *combination with other publicly available information, reveals*  
25 *the individual’s identity.*

26     (d) “Third party” means an advertising network, consumer data  
27 *reseller, data analytics provider, provider of health care, health*  
28 *care service plan, pharmaceutical company, government entity,*  
29 *operating system or platform, social network, or other commercial*  
30 *Internet Web site or online service.*

31     22596.1. (a) An operator of a commercial health monitoring  
32 *program shall not intentionally share, sell, disclose, use for*  
33 *marketing, or otherwise use health information to or with a third*  
34 *party without first obtaining explicit authorization from the*  
35 *individual. The request for authorization shall include the nature*  
36 *of the third party and the reason for the request.*

1     **(b) (1)** *An authorization is not required where the third party*  
2 *solely provides services to the operator of the commercial health*  
3 *monitoring program.*

4     **(2)** *A third party that solely provides services to the operator*  
5 *of the commercial health monitoring program shall not further*  
6 *disclose health information, subject to the authorization*  
7 *requirements of subdivision (a).*

8     **(c)** *An operator of a commercial health monitoring program*  
9 *that creates, maintains, preserves, stores, abandons, destroys, or*  
10 *disposes of health information shall do so in a manner that*  
11 *preserves the confidentiality of the health information contained*  
12 *therein.*

13     **(d)** *This section is not intended to limit the required disclosure*  
14 *of health information pursuant to another provision of law.*

15     **(e)** *Nothing in this section shall be construed to limit or*  
16 *otherwise affect existing privacy protections provided for in state*  
17 *or federal law.*

18     **22596.2. (a)** *An employer that receives health information*  
19 *shall establish appropriate procedures to ensure the confidentiality*  
20 *and protection from unauthorized use and disclosure of*  
21 *information. These procedures may include, but are not limited*  
22 *to, instruction regarding confidentiality of employees and agents*  
23 *handling files containing health information and security systems*  
24 *restricting access to files containing health information.*

25     **(b)** *An employer shall not discriminate against an employee in*  
26 *any terms or conditions of employment due to that employee's*  
27 *refusal to provide an authorization pursuant to Section 22596.1.*

28     **(c)** *An employer shall not discriminate against an employee in*  
29 *any terms or conditions of employment due to the findings of that*  
30 *employee's health information.*

31     **(d)** *An employer shall not use, disclose, or knowingly permit its*  
32 *employees or agents to use or disclose health information which*  
33 *the employer possesses pertaining to its employees without first*  
34 *obtaining authorization to do so.*

35     **(e)** *An employer that has attempted in good faith to comply with*  
36 *this section shall not be liable for any unauthorized use of the*  
37 *health information by the person or entity to which the employer*  
38 *disclosed the health information.*

1 (f) A recipient of health information pursuant to an authorization  
2 as provided by this chapter shall not further disclose that health  
3 information unless in accordance with a new authorization.

4 SECTION 1. Section 56.05 of the Civil Code is amended to  
5 read:

6 56.05. For purposes of this part:

7 (a) “Authorization” means permission granted in accordance  
8 with Section 56.11 or 56.21 for the disclosure of medical  
9 information.

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

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

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

26 (e) “Endanger” means that the subscriber or enrollee fears that  
27 disclosure of his or her medical information could subject the  
28 subscriber or enrollee to harassment or abuse.

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

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

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

1 (i) “Marketing” means to make a communication about a product  
2 or service that encourages recipients of the communication to  
3 purchase or use the product or service.

4 “Marketing” does not include any of the following:

5 (1) Communications made orally or in writing for which the  
6 communicator does not receive direct or indirect remuneration,  
7 including, but not limited to, gifts, fees, payments, subsidies, or  
8 other economic benefits, from a third party for making the  
9 communication.

10 (2) Communications made to current enrollees solely for the  
11 purpose of describing a provider’s participation in an existing  
12 health care provider network or health plan network of a  
13 Knox-Keene licensed health plan to which the enrollees already  
14 subscribe; communications made to current enrollees solely for  
15 the purpose of describing if, and the extent to which, a product or  
16 service, or payment for a product or service, is provided by a  
17 provider, contractor, or plan or included in a plan of benefits of a  
18 Knox-Keene licensed health plan to which the enrollees already  
19 subscribe; or communications made to plan enrollees describing  
20 the availability of more cost-effective pharmaceuticals.

21 (3) Communications that are tailored to the circumstances of a  
22 particular individual to educate or advise the individual about  
23 treatment options, and otherwise maintain the individual’s  
24 adherence to a prescribed course of medical treatment, as provided  
25 in Section 1399.901 of the Health and Safety Code, for a chronic  
26 and seriously debilitating or life-threatening condition as defined  
27 in subdivisions (d) and (e) of Section 1367.21 of the Health and  
28 Safety Code, if the health care provider, contractor, or health plan  
29 receives direct or indirect remuneration, including, but not limited  
30 to, gifts, fees, payments, subsidies, or other economic benefits,  
31 from a third party for making the communication, if all of the  
32 following apply:

33 (A) The individual receiving the communication is notified in  
34 the communication in typeface no smaller than 14-point type of  
35 the fact that the provider, contractor, or health plan has been  
36 remunerated and the source of the remuneration.

37 (B) The individual is provided the opportunity to opt out of  
38 receiving future remunerated communications.

39 (C) The communication contains instructions in typeface no  
40 smaller than 14-point type describing how the individual can opt

1 out of receiving further communications by calling a toll-free  
2 number of the health care provider, contractor, or health plan  
3 making the remunerated communications. No further  
4 communication may be made to an individual who has opted out  
5 after 30 calendar days from the date the individual makes the opt  
6 out request.

7 (j) “Medical information” means any individually identifiable  
8 information, in electronic or physical form, in possession of or  
9 derived from a provider of health care, health care service plan,  
10 commercial health monitoring device, pharmaceutical company,  
11 or contractor regarding a patient’s medical history, mental or  
12 physical condition, or treatment. “Individually identifiable” means  
13 that the medical information includes or contains any element of  
14 personal identifying information sufficient to allow identification  
15 of the individual, such as the patient’s name, address, electronic  
16 mail address, telephone number, or social security number, or other  
17 information that, alone or in combination with other publicly  
18 available information, reveals the individual’s identity.

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

22 (l) “Pharmaceutical company” means any company or business,  
23 or an agent or representative thereof, that manufactures, sells, or  
24 distributes pharmaceuticals, medications, or prescription drugs.  
25 “Pharmaceutical company” does not include a pharmaceutical  
26 benefits manager, as included in subdivision (e), or a provider of  
27 health care.

28 (m) “Provider of health care” means any person licensed or  
29 certified pursuant to Division 2 (commencing with Section 500)  
30 of the Business and Professions Code; any person licensed pursuant  
31 to the Osteopathic Initiative Act or the Chiropractic Initiative Act;  
32 any person certified pursuant to Division 2.5 (commencing with  
33 Section 1797) of the Health and Safety Code; any clinic, health  
34 dispensary, or health facility licensed pursuant to Division 2  
35 (commencing with Section 1200) of the Health and Safety Code.  
36 “Provider of health care” does not include insurance institutions  
37 as defined in subdivision (k) of Section 791.02 of the Insurance  
38 Code.

39 (n) “Sensitive services” means all health care services described  
40 in Sections 6924, 6925, 6926, 6927, 6928, and 6929 of the Family

1 ~~Code, and Sections 121020 and 124260 of the Health and Safety~~  
2 ~~Code, obtained by a patient at or above the minimum age specified~~  
3 ~~for consenting to the service specified in the section.~~  
4 ~~(o) “Subscriber” has the same meaning as that term is defined~~  
5 ~~in Section 1345 of the Health and Safety Code.~~  
6 ~~(p) “commercial health monitoring device” means a device~~  
7 ~~capable of connecting to the Internet that uses sensors to collect~~  
8 ~~biometric or physiologic data while in contact with the individual.~~  
9 ~~SEC. 2. No reimbursement is required by this act pursuant to~~  
10 ~~Section 6 of Article XIII B of the California Constitution because~~  
11 ~~the only costs that may be incurred by a local agency or school~~  
12 ~~district will be incurred because this act creates a new crime or~~  
13 ~~infraction, eliminates a crime or infraction, or changes the penalty~~  
14 ~~for a crime or infraction, within the meaning of Section 17556 of~~  
15 ~~the Government Code, or changes the definition of a crime within~~  
16 ~~the meaning of Section 6 of Article XIII B of the California~~  
17 ~~Constitution.~~