AMENDED IN SENATE AUGUST 19, 2016

AMENDED IN ASSEMBLY APRIL 28, 2016

AMENDED IN ASSEMBLY APRIL 11, 2016

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 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. 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.

This bill would prohibit an operator of a commercial health monitoring program from intentionally sharing, selling, or disclosing *individually identifiable* health monitoring 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 specify that an authorization is not required where monitoring a 3rd party solely provides a service to the program and does not further use or disclose health monitoring information.~~ *providing clear and conspicuous notice and obtaining the consumer's affirmative consent, as provided, and would provide that individually identifiable information may be disclosed to specified entities without consent under specified circumstances, including to a government official if necessary to prevent an emergency involving the danger of death or serious physical injury to a person, if the disclosing entity provides notice of the disclosure as soon as practicable.* The bill would also require an employer that receives health monitoring information in possession of or derived from a commercial health monitoring program to establish procedures to ~~ensure~~ *preserve* the confidentiality and security of that information, as provided. The bill would further prohibit an employer from discriminating against an employee based on an employee's health monitoring information or if that employee does not ~~authorize~~ *consent to* the use of his or her health monitoring information. The bill would exempt a covered entity, provider of health care, business associate, health care service plan, contractor, employer, or any other person subject to the federal Health Insurance Portability and Accountability

Act of 1996 (HIPAA) or the Confidentiality of Medical Information Act from these requirements.

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

Chapter 22.4. Digital Commercial Health Monitoring Programs

22596. For purposes of this chapter:

(a) "Commercial health monitoring program" means a commercial Internet Web ~~site or online service used by consumers that collects health monitoring information regarding the consumer's mental or physical condition from sources including, but not limited to, manual entry, sensors, or both.~~ *site, online service, or product used by consumers whose primary purpose is to collect the consumer's individually identifiable health monitoring information.*

(b) "Consumer" includes, but is not limited to, employees of employers subject to the provisions of Section 22596.2.

(c) "Health care provider" has the meaning given that term in the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA) (Public Law 104-191).

~~(b)~~

(d) "Health monitoring information" means ~~any individually identifiable~~ information, in electronic or physical form, ~~in possession of, or derived from, a commercial health monitoring program regarding a consumer's mental or physical condition.~~ *about a consumer's mental or physical condition that is collected by a commercial health monitoring program through a direct measurement of a consumer's mental or physical condition or though user-input regarding a consumer's mental or physical condition into a commercial health monitoring program.*

~~(c)~~

(e) "Individually identifiable" means ~~that the health monitoring~~ information *that* includes or contains an element of personal identifying information sufficient to allow identification of the consumer, including, but not limited to, the consumer's name, address, electronic mail address, telephone number, social security number, or unique electronic identifier, or other information that, alone or in combination with other publicly available information, reveals the consumer's identity.

~~(d) "Third party" includes, but is not limited to, an advertising network, consumer data reseller, data analytics provider, health care service plan, pharmaceutical company, government entity, operating system or platform, social network, or other commercial Internet Web site or online service.~~

~~(e) "Consumer" includes employees of employers subject to the provisions of Section 22596.2.~~

~~(f) "Business associate" means a person or entity who provides, other than in the capacity of a member of the workforce of an operator of a commercial health monitoring program, legal, actuarial, accounting, consulting, data aggregation (as defined in the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA) (Public Law 104-191)), management, administrative, accreditation, or financial services to or for a consumer health monitoring program where the provision of the service involves the disclosure of health monitoring information from a commercial health monitoring program or from another business associate of a commercial health monitoring program.~~

(f) "Service provider" means an entity that does not further use or disclose individually identifiable health information except at the direction of the commercial health monitoring program to other service providers of the commercial health monitoring programs and does either of the following:

(1) Provides services to the operator, or on behalf of the operator, of the commercial health monitoring program that solely support the functionality or operation of the commercial health monitoring program.

(2) Controls, is controlled by, or is under common control with the provider of the commercial health monitoring program where both of the following apply:

(A) The entity maintains third-party data sharing practices, with respect to individually identifiable health monitoring

information, that are at least as protective of privacy as those of the commercial health monitoring program.

(B) The operator of the commercial health monitoring program disclosing the individually identifiable health monitoring information and the entity receiving the individually identifiable health monitoring information are both principally engaged in the same line of business.

(g) "Third party" means an entity that is not a service provider, with whom the consumer does not have a direct relationship with respect to the consumer's use of the commercial health monitoring program, and whose processing of individually identifiable health monitoring information is not otherwise necessary for the functionality of the commercial health monitoring program.

22596.1. (a) An operator of a commercial health monitoring program shall not intentionally share, sell, or disclose *individually identifiable* health monitoring information to or with a third party without first ~~obtaining from the consumer explicit opt-in authorization which~~ *providing clear and conspicuous notice and obtaining the consumer's affirmative consent that* fulfills the following requirements:

(1) The request for ~~authorization shall be clear, conspicuous, and~~ *consent shall be* separate from all other authorizations or agreements.

(2) The request for ~~authorization~~ *consent* shall include the name ~~and~~ *or* nature of the third party and the ~~reason~~ *purpose* for the request.

~~(3) Each request for authorization shall be limited to a single third-party entity.~~

~~(4)~~

(3) (A) A consumer's refusal to ~~authorize third-party~~ *consent to third-party sharing, sale, or* disclosure of *individually identifiable* health monitoring information shall not limit the consumer's ability to use the commercial health monitoring program even if features and services provided by the specific third party are inoperable.

~~(5) A waiver of any legal right, penalty, remedy, forum, or enforcement procedure imposed as a condition of use is unconscionable and unenforceable. Any person who seeks to enforce such a waiver shall have the burden of proving that the~~

~~waiver was knowing and voluntary and was not made as a condition of use.~~

~~(6) Each request for authorization shall state that a consumer has the right to revoke the authorization at any time without cost or penalty by a readily accessible method.~~

~~(b) Notwithstanding subdivision (a), an authorization is not required where the third party solely provides services to the operator of the commercial health monitoring program and does not further use or disclose health monitoring information.~~

(B) This paragraph does not apply if the primary function of the commercial health monitoring program is the sharing, sale, or disclosure of individually identifiable health monitoring information to third parties and the consumer is notified of this function at the time of the request for consent.

(4) A waiver of any legal right, penalty, remedy, forum, or enforcement procedure presented to the consumer in the consent described by this section is unenforceable and void as a matter of law.

(b) An operator of a commercial health monitoring program shall make available and provide notice of a process whereby a consumer may withdraw the consent granted in subdivision (a) though the notice does not expressly need to be included in the consent described in subdivision (a). Any withdrawal of consent shall apply prospectively and shall not impact valid disclosures and consent prior to the operative date of withdrawal.

(c) Where health monitoring information is stored in an individually identifiable manner, upon request by the consumer, the operator of the commercial health monitoring program shall delete or provide to the consumer his or her individually identifiable health monitoring information. A commercial health monitoring program may assess a reasonable administrative charge for the cost of accessing, copying, or deleting individually identifiable health monitoring information under this chapter.

~~(c)~~

(d) An operator of a commercial health monitoring program that creates, maintains, preserves, stores, abandons, *deletes,* destroys, or disposes of health monitoring information shall do so in a manner ~~that preserves~~ *to preserve* the security and confidentiality of the *individually identifiable* health monitoring information contained therein.

~~(d)~~

(e) This chapter is not intended to limit the required disclosure of *individually identifiable* health monitoring information pursuant to another provision of law.

~~(e)~~

(f) Nothing in this chapter shall be construed to limit or otherwise reduce existing privacy protections provided for in state or federal law.

~~(f) Health monitoring information may be disclosed to a provider of health care or other health care professional or facility to aid the diagnosis or treatment of the consumer, where the consumer is unable to authorize the disclosure due to an emergent medical condition.~~

(g) Individually identifiable health monitoring information may be disclosed to the following persons without satisfying the consent requirements of this chapter if the disclosing entity provides notice of the disclosure to the consumer whose individually identifiable health monitoring information was disclosed as soon as practicable:

(1) To a health care provider to aid in the diagnosis or treatment of the consumer, where the consumer is unable to consent to the disclosure due to an emergent medical condition.

(2) To a government official if necessary to prevent an emergency involving danger of death or serious physical injury to a person, that requires access to the individually identifiable commercial health information.

(h) A recipient of individually identifiable health monitoring information that is not a commercial health monitoring program shall not further disclose that health monitoring information. Responsibility for a violation of this paragraph shall not rest with the commercial health monitoring agency but with the disclosing entity.

22596.2. (a) An employer that receives health monitoring information shall establish appropriate procedures to ~~ensure~~ *preserve* the security and confidentiality of information. These procedures may include, but are not limited to, instruction regarding confidentiality of employees and agents handling files containing health monitoring information and security systems restricting access to files containing ~~health monitoring~~ *that* information.

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

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

(d) An employer shall not use, disclose, or knowingly permit its employees or agents to use or disclose *individually identifiable* health monitoring information ~~which~~ *that* the employer possesses pertaining to its employees without first obtaining ~~authorization to do so.~~ *that employee's consent to do so pursuant to Section 22596.*

(e) An employer that has ~~attempted in good faith to comply~~ *complied* with this section shall not be liable for any unauthorized use or disclosure of ~~the~~ *individually identifiable* health monitoring ~~information by the person or entity to which the employer disclosed the health monitoring~~ information.

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

(f) An entity that is not a commercial health monitoring program that receives individually identifiable health monitoring information from an employer shall not further disclose that health monitoring information. Responsibility for a violation of this paragraph shall not rest with commercial health monitoring program or with the employer but with the disclosing entity.

22596.3. (a) A covered entity, provider of health care, business associate, health care service plan, contractor, employer, or any other person subject to the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA) (Public Law ~~104–191)~~ *104-191)* or the Confidentiality of Medical Information Act (Part 2.6 (commencing with Section 56) of Division 1 of the Civil Code) shall not be subject to this chapter with respect to any activity *or exemption* regulated by those acts.

(b) The definitions in those acts, in effect on January 1, 2016, shall apply to this section.

O