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, 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. *The bill would exempt a covered entity, provider of health care, business entity, health care service plan, contractor, employer, or any other person subject to and compliant with the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA) and 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 information regarding an individual's mental or physical condition from sources including, but not limited to, manual entry, sensors, or both.

(b) "Health information" mean 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.

(c) "Individually identifiable" means that the health information includes or contains an element of personal identifying information sufficient to allow identification of the individual, including, but not limited to, the individual'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 individual's identity.

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

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

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

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

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

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

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

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

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

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

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

22596.3. (a) A covered entity, provider of health care, business entity, health care service plan, contractor, employer, or any other person subject to and compliant with the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA) (P.L. 104–191) and 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.

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

O