AMENDED IN ASSEMBLY APRIL 21, 2014

CALIFORNIA LEGISLATURE—2013–14 REGULAR SESSION

ASSEMBLY BILL No. 1830

Introduced by Assembly Member Conway
(Coauthors: Assembly Members Hagman, Harkey, Olsen, Wagner, and Wilk)

February 18, 2014

An act to add Section 100509 to the Government Code, relating to health care coverage.

LEGISLATIVE COUNSEL'S DIGEST

AB 1830, as amended, Conway. California Health Benefit Exchange: confidentiality of personally identifiable information.

Existing law, the federal Patient Protection and Affordable Care Act (PPACA), requires each state to establish an American Health Benefit Exchange by January 1, 2014, that makes available qualified health plans to qualified individuals and small employers. PPACA prohibits an Exchange from using or disclosing the personally identifiable information it creates or collects other than to the extent necessary to carry out specified functions. Existing law also requires an Exchange to establish and implement privacy and security standards that are consistent with specified principles and to require the same or more stringent privacy and security standards as a condition of contract or agreement with individuals or entities. A person who knowingly and willfully uses or discloses information in violation of PPACA is subject to a civil penalty of no more than $25,000 per person or entity, per use or disclosure, in additional to any other penalties prescribed by law.

Existing state law establishes the California Health Benefit Exchange within state government, specifies the powers and duties of the board

governing the Exchange, and requires the board to facilitate the purchase of qualified health plans through the Exchange by qualified individuals and small employers by January 1, 2014. Existing law requires the board to employ necessary staff and authorizes the board to enter into contracts. Under existing law, the board of the Exchange is required to submit fingerprint images to the Department of Justice for all employees, prospective employees, contractors, subcontractors, volunteers, or vendors of the Exchange whose duties include access to specified personal information for the purposes of obtaining state or federal conviction records, as specified.

This bill would, where the Exchange creates or collects personally identifiable information for the purpose of determining eligibility for specified plans and programs, authorize the Exchange to use or disclose that information only to the extent necessary to carry out specified functions authorized under PPACA *or to carry out other nonspecified functions that satisfy certain federal criteria. The bill would require the Exchange to establish and implement privacy and security standards that are consistent with specified principles and to execute a contract with a non-Exchange entity that contains various provisions, including a provision requiring the non-Exchange entity to comply with the same privacy and security standards and to bind any downstream entity to those privacy and security standards*. The bill would prohibit a contractor, subcontractor, volunteer, or vendor of the Exchange who gains access to personally identifiable information in the course of fulfilling his, her, or its duties as a contractor, subcontractor, volunteer, or vendor from using or disclosing that information other than to the extent necessary to carry out those duties*, except as specified*. ~~The bill would require a contractor, subcontractor, volunteer, or vendor of the Exchange to comply with the privacy and security standards adopted by the Exchange pursuant to PPACA.~~ An individual or entity who knowingly and willfully violates ~~these~~ *the bill's disclosure* provisions would be subject to a civil penalty of not more than $25,000 per individual or entity, per use or disclosure, in addition to any other penalties prescribed by law.

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

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

SECTION 1. Section 100509 is added to the Government Code, to read:

100509. (a) (1) Where the Exchange creates or collects personally identifiable information for the purpose of determining eligibility for enrollment in a qualified health plan, determining eligibility for other insurance affordability programs, as defined in Section 155.20 of Title 45 of the Code of Federal Regulations, or determining eligibility for exemptions from the individual responsibility provisions in Section 5000A of the federal Internal Revenue Code, the Exchange may only use or disclose the information to the extent necessary to carry out the functions described in Section 155.200 of Title 45 of the Code of Federal Regulations *or to carry out the functions not described in Section 155.200 of Title 45 of the Code of Federal Regulations that satisfy Section 155.260(a)(1)(ii) or (iii) of Title 45 of the Code of Federal Regulations*.

(2) The Exchange shall not create, collect, use, or disclose personally identifiable information~~ while fulfilling its responsibilities in accordance with this title and Section 155.200 of Title 45 of the Code of Federal Regulations~~ unless the creation, collection, use, or disclosure is consistent with Section 155.260 of Title 45 of the Code of Federal Regulations.

(3) The Exchange shall establish and implement privacy and security standards that are consistent with the principles listed in Section 155.260(a)(3) of Title 45 of the Code of Federal Regulations.

~~(3)~~

(4) For purposes of this subdivision, "Exchange" includes a member of the board or staff of the Exchange.

(b) Prior to becoming a non-Exchange entity, the Exchange shall execute a contract with the entity that includes all of the following:

(1) A description of the functions to be performed by the non-Exchange entity.

(2) A provision requiring the non-Exchange entity to comply with the privacy and security standards adopted by the Exchange pursuant to subdivision (c), and specifically listing or incorporating those standards.

(3) A provision requiring the non-Exchange entity to monitor, periodically assess, and update its security controls and related system risks to ensure the continued effectiveness of those controls in accordance with Section 155.260(a)(5) of Title 45 of the Code of Federal Regulations.

(4) A provision requiring the non-Exchange entity to inform the Exchange of any change in its administrative, technical, or operational environments defined as material within the contract.

(5) A provision that requires the non-Exchange entity to bind any downstream entities to the same privacy and security standards and obligations to which the non-Exchange entity has agreed in its contract or agreement with the Exchange under paragraph (2).

(c) When the collection, use, or disclosure of personally identifiable information is not otherwise required by law, the privacy and security standards to which the Exchange shall bind a non-Exchange entity shall meet all of the following requirements:

(1) Be consistent with the principles and requirements listed in Section 155.260(a)(1) to (6), inclusive, of Title 45 of the Code of Federal Regulations.

(2) Comply with Section 155.260(c), (d), (f), and (g) of Title 45 of the Code of Federal Regulations.

(3) Take into consideration all of the following:

(A) The environment in which the non-Exchange entity is operating.

(B) Whether the standards are relevant and applicable to the non-Exchange entity's duties and activities in connection with the Exchange.

(C) Any existing legal requirements to which the non-Exchange entity is bound in relation to its administrative, technical, and operational controls and practices, including, but not limited to, its existing data handling and information technology processes and protocols.

~~(b)~~

(d) A contractor, subcontractor, volunteer, or vendor of the Exchange who gains access to personally identifiable information in the course of fulfilling his, her, or its duties as a contractor, subcontractor, volunteer, or vendor of the Exchange shall not use or disclose that information other than to the extent necessary to carry out those duties. *This subdivision shall not apply to a contractor, subcontractor, volunteer, or vendor of the Exchange*

who is a covered entity under the federal Health Insurance Portability and Accountability Act and the regulations issued pursuant to Part C of that act (45 C.F.R. Parts 160 and 164), provided that the contractor, subcontractor, volunteer, or vendor otherwise complies with those federal laws and any other requirements applicable to the contractor, subcontractor, volunteer, or vendor pursuant to this section.

~~(c) A contractor, subcontractor, volunteer, or vendor of the Exchange shall comply with the privacy and security standards adopted by the Exchange pursuant to Section 155.260 of Title 45 of the Code of Federal Regulations.~~

~~(d)~~

(e) This section does not apply when the use or disclosure of personally identifiable information is otherwise compelled by judicial or administrative process or by any other provision of law, except as otherwise provided in the federal act.

~~(e)~~

(f) Where the Exchange or a ~~contractor, subcontractor, volunteer, or vendor of the Exchange~~ *non-Exchange entity* has access to federal tax return information, that information shall be kept confidential and disclosed, used, and maintained only in accordance with Section 6103 of the federal Internal Revenue Code.

~~(f)~~

(g) An individual or entity who knowingly and willfully violates ~~this section~~ *subdivision (a) or (d)* shall be subject to a civil penalty of not more than twenty-five thousand dollars ($25,000) per individual or entity, per use or disclosure, in addition to any other penalties prescribed by law.

~~(g)~~

(h) For purposes of this section, ~~"personally~~ *the following definitions shall apply:*

(1) "Non-Exchange entity" means an individual or entity that does either of the following:

(A) Gains access to personally identifiable information submitted to the Exchange.

(B) Collects, uses, or discloses personally identifiable information gathered directly from applicants, qualified individuals, or enrollees while that individual or entity is performing functions agreed to with the Exchange.

(2) "*Personally* identifiable information" means information that includes or contains any 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, credit card number, place or date of birth, biometric records, or other information that, alone or in combination with other publicly available information, reveals the individual's identity.

O