

Assembly Bill No. 1541

CHAPTER 96

An act to amend Section 1798.81.5 of the Civil Code, relating to privacy.

[Approved by Governor July 14, 2015. Filed with
Secretary of State July 14, 2015.]

LEGISLATIVE COUNSEL'S DIGEST

AB 1541, Committee on Privacy and Consumer Protection. Privacy: personal information.

Existing law requires a business that owns, licenses, or maintains personal information about a California resident to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure. Existing law defines terms for purposes of this law, including "personal information."

This bill would revise the definition of personal information to include health insurance information, as defined, and a username or email address combined with a password or security question and answer for access to an online account.

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

SECTION 1. Section 1798.81.5 of the Civil Code is amended to read:

1798.81.5. (a) (1) It is the intent of the Legislature to ensure that personal information about California residents is protected. To that end, the purpose of this section is to encourage businesses that own, license, or maintain personal information about Californians to provide reasonable security for that information.

(2) For the purpose of this section, the terms "own" and "license" include personal information that a business retains as part of the business' internal customer account or for the purpose of using that information in transactions with the person to whom the information relates. The term "maintain" includes personal information that a business maintains but does not own or license.

(b) A business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.

(c) A business that discloses personal information about a California resident pursuant to a contract with a nonaffiliated third party that is not

subject to subdivision (b) shall require by contract that the third party implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.

(d) For purposes of this section, the following terms have the following meanings:

(1) “Personal information” means either of the following:

(A) An individual’s first name or first initial and his or her last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted:

(i) Social security number.

(ii) Driver’s license number or California identification card number.

(iii) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual’s financial account.

(iv) Medical information.

(v) Health insurance information.

(B) A username or email address in combination with a password or security question and answer that would permit access to an online account.

(2) “Medical information” means any individually identifiable information, in electronic or physical form, regarding the individual’s medical history or medical treatment or diagnosis by a health care professional.

(3) “Health insurance information” means an individual’s insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual’s application and claims history, including any appeals records.

(4) “Personal information” does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(e) The provisions of this section do not apply to any of the following:

(1) A provider of health care, health care service plan, or contractor regulated by the Confidentiality of Medical Information Act (Part 2.6 (commencing with Section 56) of Division 1).

(2) A financial institution as defined in Section 4052 of the Financial Code and subject to the California Financial Information Privacy Act (Division 1.2 (commencing with Section 4050) of the Financial Code).

(3) A covered entity governed by the medical privacy and security rules issued by the federal Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Availability Act of 1996 (HIPAA).

(4) An entity that obtains information under an agreement pursuant to Article 3 (commencing with Section 1800) of Chapter 1 of Division 2 of the Vehicle Code and is subject to the confidentiality requirements of the Vehicle Code.

(5) A business that is regulated by state or federal law providing greater protection to personal information than that provided by this section in regard to the subjects addressed by this section. Compliance with that state or federal law shall be deemed compliance with this section with regard to those subjects. This paragraph does not relieve a business from a duty to comply with any other requirements of other state and federal law regarding the protection and privacy of personal information.

O