SENATE JUDICIARY COMMITTEE
Senator Thomas Umberg, Chair
2021-2022 Regular Session

AB 1436 (Chau)
Version: June 21, 2021
Hearing Date: June 29, 2021
Fiscal: Yes
Urgency: No
CK

SUBJECT

Information privacy: digital health feedback systems

DIGEST

This bill makes a business a provider of health care, and therefore subject to California's Confidentiality of Medical Information Act (CMIA), when it offers to a consumer personal health record system software or hardware that is designed to maintain and make available personal health record system information for purposes of allowing the individual to manage their information, or for the diagnosis, treatment, or management of a medical condition of the individual.

EXECUTIVE SUMMARY

Existing California and federal law strictly govern the use of a patient's medical information. These statutory frameworks favor the privacy of the patient, with caveats for the sharing of medical information when necessary for treatment. California's CMIA allows adult patients in California to keep personal health information confidential and decide whether and when to share that information. CMIA protects "medical information," and restricts its disclosure by "providers of health care" and "health care service plans," as defined and specified.

The use of digital health products and services that collect and transmit certain health data raises serious privacy concerns. This bill defines "personal health record system" (PHRS) as a commercial internet website, online service, or product that is used by an individual and that collects the individual's personal health record information. It deems a business that offers PHRS software or hardware a "provider of health care" and subjects it to the provisions of CMIA.

The bill is sponsored by the author and supported by various consumer and privacy groups, including Consumer Reports and ACLU California Action. It is opposed by

various industry groups, including the Masimo Corporation. If the bill passes this Committee, it will then go to the Senate Health Committee.

PROPOSED CHANGES TO THE LAW

Existing federal law:

1) Establishes the Health Insurance Portability and Accountability Act (HIPAA), which provides privacy protections for patients' protected health information and generally prohibits a covered entity, as defined (health plan, health care provider, and health care clearing house), from using or disclosing protected health information except as specified or as authorized by the patient in writing. (45 C.F.R. § 164.500 et seq.)

2) Provides that if HIPAA's provisions conflict with a provision of state law, the provision that is the most protective of patient privacy prevails. (45 C.F.R. § 164.500 et seq.)

Existing state law:

1) Provides, pursuant to the California Constitution, that all people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy. (Cal. Const., art. I, § 1.)

2) Establishes the CMIA, which establishes protections for the use of medical information. (Civ. Code § 56 et seq.)

3) Prohibits providers of health care, health care service plans, or contractors, as defined, from sharing medical information without the patient's written authorization, subject to certain exceptions. (Civ. Code § 56.10.)

4) Provides that every provider of health care, health care service plan, pharmaceutical company, or contractor who creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information shall do so in a manner that preserves the confidentiality of the information contained therein. Any provider of health care, health care service plan, pharmaceutical company, or contractor who negligently creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information shall be subject to remedies and penalties, as specified. (Civ. Code § 56.101.)

5) Defines "patient," for purposes of CMIA, to mean any natural person, whether or not still living, who received health care services from a provider of health care and to whom medical information pertains. (Civ. Code § 56.05(k).)

6) Defines "medical information," for purposes of CMIA, to mean any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care, health care service plan, pharmaceutical company, or contractor regarding a patient's medical history, mental or physical condition, or treatment. "Individually identifiable" means that the medical information includes or contains any element of personal identifying information sufficient to allow identification of the individual, such as the patient's name, address, electronic mail address, telephone number, or social security number, or other information that, alone or in combination with other publicly available information, reveals the individual's identity. (Civ. Code § 56.05(j).)

7) Defines "health care service plan" to mean any entity regulated pursuant to the Knox-Keene Health Care Service Plan Act of 1975. (Civ. Code § 56.05(g).)

8) Defines a "licensed health care professional," for purposes of CMIA, to mean any person licensed or certified pursuant to the Business and Professions Code, the Osteopathic Initiative Act or the Chiropractic Initiative Act, or the Health and Safety Code, as specified. (Civ. Code § 56.05(h).)

9) Defines "provider of health care," for purposes of CMIA, to mean any person licensed or certified pursuant to the Business and Professions Code, as specified; the Osteopathic Initiative Act or the Chiropractic Initiative Act; the Health and Safety Code, as specified; or any licensed clinic, health dispensary, or health facility, as specified. The term does not include insurance institutions, as defined. (Civ. Code § 56.05(m).)

10) Provides that any business organized for the purpose of maintaining medical information in order to make the information available to an individual or to a provider of health care at the request of the individual or the provider of health care, for purposes of allowing the individual to manage his or her information, or for the diagnosis and treatment of the individual, shall be deemed to be a provider of health care subject to the requirements of CMIA. (Civ. Code § 56.06(a).)

11) Provides that any business that offers software or hardware to consumers, including a mobile application or other related device that is designed to maintain medical information in order to make the information available to an individual or a provider of health care at the request of the individual or a provider of health care, for purposes of allowing the individual to manage their information, or for the diagnosis, treatment, or management of a medical condition of the individual, shall be deemed to be a provider of health care subject to the requirements of CMIA. (Civ. Code § 56.06(b).)

12) Provides that any business that is licensed pursuant to the Medicinal and Adult-Use Cannabis Regulation and Safety Act that is authorized to receive or receives identification cards or information contained in a physician's recommendation, as provided, shall be deemed to be a provider of health care subject to the requirements of CMIA. (Civ. Code § 56.06(c).)

13) Provides that any business described in the preceding three paragraphs must maintain the same standards of confidentiality required of a provider of health care with respect to medical information disclosed to the business. Such businesses are subject to the penalties for improper use and disclosure of medical information prescribed in CMIA. (Civ. Code § 56.06(d)-(e).)

14) Provides that any provider of health care, a health care service plan, pharmaceutical company, or contractor who negligently creates, maintains, preserves, stores, abandons, destroys, or disposes of written or electronic medical records shall be subject to damages in a civil action or an administrative fine, as specified. (Civ. Code § 56.36.)

This bill:

1) Defines "personal health record system" as a commercial internet website, online service, or product that is used by an individual and that collects the individual's personal health record information.

2) Defines "personal health record information" to mean individually identifiable information, in electronic or physical form, about an individual's mental or physical condition that is collected by a personal health record system through a direct measurement of an individual's mental or physical condition or through user input regarding an individual's mental or physical condition into a personal health record system.

3) Includes personal health record information in the definition of "medical information" in CMIA.

4) Provides that any business that offers personal health record system software or hardware to a consumer, including a mobile application or other related device that is designed to maintain personal health record system information, as defined in subdivision (m) of Section 56.05, in order to make information available to an individual or to a provider of health care at the request of the individual or provider of health care, for purposes of allowing the individual to manage their information, or for the diagnosis, treatment, or management of a medical condition of the individual, shall be deemed to be a provider of health care subject to the requirements of this part.

COMMENTS

1. Protections for medical information

HIPAA, enacted in 1996, guarantees privacy protection for individuals with regards to specific health information. (Pub.L. 104–191, 110 Stat. 1936.) Generally, protected health information is any information held by a covered entity which concerns health status, provision of healthcare, or payment for healthcare that can be connected to an individual. HIPAA privacy regulations require healthcare providers and organizations to develop and follow procedures that ensure the confidentiality and security of personal health information when it is transferred, received, handled, or shared. HIPAA further requires reasonable efforts when using, disclosing, or requesting protected health information, to limit disclosure of that information to the minimum amount necessary to accomplish the intended purpose.

CMIA (Civ. Code § 56 et seq.) allows adult patients in California to keep personal health information confidential and decide whether and when to share that information. These provisions are guided to protect Californians' fundamental right to privacy. (Cal. Const., art. I, § 1.) CMIA protects "medical information," and generally regulates what providers of health care, and health care service plans, can do with such information.

2. Extending existing protections to sensitive medical information

In November 2017, the Federal Drug Administration (FDA) approved its first digital drug.[1] The drug came in the form of a pill with an embedded sensor that has the capability to determine and transmit whether someone has taken it. The sensor inside this pill is the size of a grain of sand and detects and records when it is ingested, sending that information to a patch worn by the patient. The patch thereafter transmits the information to an application that can be downloaded to a smartphone.

Along these same lines, the FDA cleared the way for new digitally enhanced inhalers. Sensors are attached to patients' inhalers, and they "deliver insights on medication use to [an app] on their smartphone, which patients can then share with their clinician to help inform their treatment plan."[2]

---

[1] News Release, *FDA approves pill with sensor that digitally tracks if patients have ingested their medication* (November 13, 2017) FDA, https://www.fda.gov/news-events/press-announcements/fda-approves-pill-sensor-digitally-tracks-if-patients-have-ingested-their-medication#:~:text=The%20U.S.%20Food%20and%20Drug,that%20the%20medication%20was%20taken.. All internet citations are current as of June 22, 2021.

[2] Press Release, *Propeller Health Receives FDA Clearance to Connect Patients Using the Symbicort® Inhaler to its Digital Health Platform* (May 26, 2020) Businesswire, https://www.businesswire.com/news/home/20200526005068/en/Propeller-Health-Receives-FDA-Clearance-to-Connect-Patients-Using-the-Symbicort%C2%AE-Inhaler-to-its-Digital-Health-Platform.

As with many technological advances and innovations, these breakthroughs come with serious concerns about privacy. These pills and inhalers are just a couple examples of emerging technology that assists medical professionals and consumers in addressing health care concerns; others include fitness applications, advanced medical software, and other digital health products. This bill provides protections for the information collected by these various products and services by making businesses that offer them "providers of health care" thereby subjecting them to the mandates of CMIA.

This bill defines PHRS as a commercial internet website, online service, or product that is used by an individual and that collects the individual's personal health record information. Personal health record information is the individually identifiable information, in electronic or physical form, about an individual's mental or physical condition that is collected by a personal health record system through a direct measurement of an individual's mental or physical condition or through user input regarding an individual's mental or physical condition into a personal health record system.

Providers of health care are subject to various requirements under CMIA. They are prohibited from sharing medical information without the patient's written authorization, subject to certain exceptions. (Civ. Code § 56.10.) A provider of health care who creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information is required to do so in a manner that preserves the confidentiality of the information contained therein. Any provider of health care who negligently creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information is subject to certain penalties. (Civ. Code § 56.101.) If a provider negligently creates, maintains, preserves, stores, abandons, destroys, or disposes of written or electronic medical records, they are subject to damages in a civil action or an administrative fine, as specified. (Civ. Code § 56.36.)

In order to bring PHRS and attendant information within the scope of protections of CMIA, this bill makes businesses offering PHRS software or hardware, "providers of health care" and thereby subjects them to CMIA. The type of offerings would include a mobile application or other device that is intended to maintain this information with the intent to make it available to an individual or a health care provider, at their request, for the purpose of managing the data or using it for diagnosis, treatment, or management of medical conditions.

3. Building on previous legislation

This bill models AB 658 (Calderon, Ch. 296, Stats. 2013), which responded to other digital tools entering the healthcare space. Similar to this bill, AB 658 was motivated by privacy concerns connected to internet-based applications that allowed individuals to gather, store, manage, and in some cases share, personal health information. It inserted the following provision into CMIA:

> Any business that offers software or hardware to consumers, including a mobile application or other related device that is designed to maintain medical information, as defined in subdivision (g) of Section 56.05, in order to make the information available to an individual or a provider of health care at the request of the individual or a provider of health care, for purposes of allowing the individual to manage his or her information, or for the diagnosis, treatment, or management of a medical condition of the individual, shall be deemed to be a provider of health care subject to the requirements of this part. However, nothing in this section shall be construed to make a business specified in this subdivision a provider of health care for purposes of any law other than this part, including laws that specifically incorporate by reference the definitions of this part.

The provision applies to software or hardware that maintains "medical information," as defined in CMIA. The definition is limited to information "in possession of or derived from a provider of health care, health care service plan, pharmaceutical company, or contractor." As the PHRS at issue here collect information directly from consumers, the information is arguably not "medical information," as defined. To ensure the protective umbrella of CMIA covers this information, the bill makes clear that CMIA covers digital health tools that collect sensitive information from individuals, even where the information is not "in possession of or derived from a provider of health care, health care service plan, pharmaceutical company, or contractor."

In response to concerns that the bill will increase costs and hinder the development of health-related products, the author points to AB 658, which was enacted eight years ago:

> California law currently subjects a business that offers software or hardware to consumers that is designed to maintain medical information or for the diagnosis, treatment, or management of a medical condition, to CMIA. If businesses who have for years taken a similar digital approach to collecting health information can comply with CMIA, then these new digital health products and the businesses who develop them can certainly comply with CMIA without being burdened. The information they collect is unquestionably health information, so our medical privacy laws should apply to them.

Pulling the businesses that offer the software and hardware that tap into this sensitive information into the ambit of CMIA is arguably a good next step in protecting consumers' and patients' medical privacy.

4. Stakeholder positions

According to the author:

> The Covid-19 pandemic's spread through our state and the nation has profoundly impacted our society and the health care system. Health Care professionals are looking to explore any and all available tools to address this crisis. As such we can expect a greater use of digital health products, giving health care providers new ways to get useful and accurate information about their patients. Digital health products include an FDA approved digital and mobile connected inhaler that can detect when the device is used, measure the strength of the user's inhalation, and transmit this information to the user's doctor. They also include several forms of "digital pills" that are already in use. These pills combine ingestible microchip sensors with pharmaceuticals and communicate with a "patch" that collects information and sends it to an app, similar to a Fitbit. These products can record when, and in what quantity a drug is consumed, as well as the physical state of the person taking the drug, such as temperature, activity level, and heart rate. Normally, if this information was collected by a health professional it would be considered "medical information" and covered by existing medical privacy laws. However, because this information is generated or collected by a digital health app, meaning at the patient level and outside of a medical facility, it will not necessarily be captured under the existing definition of medical information. Appropriate guardrails are necessary to protect privately-collected information with an expectation of privacy. With health information privacy in a period of flux because of the pandemic, striking an appropriate balance between broadened access to health information for the public good and protection of the fundamental right to privacy requires baseline protections for medical privacy from which to work that are intuitive and consistent. AB 1436 will bring these technologies and the information they collect under California's Confidentiality of Medical Information Act by providing that any business that offers such an app or device to a consumer shall be considered a provider of healthcare. This will ensure that sensitive health data are treated with the same care as data that are generated in a traditional medical setting, and prohibit that information from being shared without the individual's written consent.

A coalition of consumer and privacy groups, including the Electronic Frontier Foundation and the Electronic Privacy Information Center write in support of the bill:

> In California, patient privacy is protected by […] CMIA and […] HIPAA. However, combined, these two laws only protect sensitive health information that is generated by healthcare providers, insurers and health

> plans, pharmaceutical companies, healthcare clearinghouses and businesses organized for the purpose of maintaining medical information. The information created by new health technology, such as digital health feedback systems and online health services, do not fall into this rubric.
>
> Drafters of these laws did not anticipate future technology that would facilitate personal health information being generated by technology outside the traditional care setting and by the patients themselves. That future, however, is here and our state laws must keep pace. Although the California Consumer Privacy Act (CCPA) would apply to this data, the law does not protect consumer data to the same extent as the medical privacy laws, creating an uneven privacy plane between health information collected by new health technology versus data created by providers and insurers and plans themselves. For example, whereas the CCPA permits data sharing but requires access, deletion, and limits on the sale of data to third parties upon request, the CMIA and HIPAA prohibit most cases of sharing at all.
>
> This bill adds certainty for patients that using new health technology will not jeopardize their privacy and potentially impact them in other areas of their lives.

Writing in opposition, a coalition of industry groups, including the California Chamber of Commerce, Internet Association, Silicon Valley Leadership Group, and the California Manufacturers & Technology Association argue:

> AB 1436 is overbroad, turning commonplace fitness trackers, basic household devices, and social media websites into medical devices. AB 1436 as drafted will affect products ranging from fitness wearables to insulin glucose monitors for people with diabetes and will have a disruptive impact on the current market for these products by drastically expanding the scope of businesses that are subject to penalties and prosecution under the Confidentiality of Medical Information Act (CMIA). This bill applies to every website, online service, or product (whether software or hardware) designed to maintain individually identifiable information about an individual's mental or physical condition. Accordingly, this definition includes virtually every digital health device or service, including digital scales, fitness wearables, blood sugar monitors, thermometers, fitness tracking tools, and wearable fitness devices. This definition is so broad that it also includes any website where individuals can post information about their health, such as their weight, or information about their mental condition, such as an online happiness/mood diary. It would also include gyms that track a client's heart rate, body fat, or measurements online, and even connected home

> treadmills and workout equipment. A company that helps consumers track their heart rate while exercising should not be subject to this complicated set of laws meant to govern health care providers who record information about abortions, sexually transmitted diseases, and psychiatric disorders. The same level of regulation is simply not warranted.

SUPPORT

ACLU California Action
Consumer Reports
Electronic Frontier Foundation
Electronic Privacy Information Center
Media Alliance
Oakland Privacy
Privacy Rights Clearinghouse

OPPOSITION

Advanced Medical Technology Association
California Chamber of Commerce
California Manufacturers & Technology Association
Civil Justice Association of California
Entertainment Software Association
Insights Association
Internet Association
Masimo Corporation
National Payroll Reporting Consortium
Silicon Valley Leadership Group
State Privacy and Security Coalition, Inc.
TechNet

RELATED LEGISLATION

Pending Legislation:

AB 1252 (Chau, 2021) is nearly identical to the current bill. It was opposed by a number of technology and medical device associations, including the Advanced Medical Technology Association, the California Chamber of Commerce, and TechNet. The bill is on the Assembly Floor.

Prior Legislation:

AB 2280 (Chau, 2020) was identical to AB 1252. It was not heard in the Senate Judiciary Committee due to the COVID-19 pandemic.

AB 384 (Chau, 2019) would have defined "personal health record" as an FDA-approved commercial internet website, online service, or product that is used by an individual at the direction of a provider of health care with the primary purpose of collecting the individual's individually identifiable personal health record information. This would have ensured that CMIA applied to information derived from or in the possession of these systems. AB 384 died in the Senate Appropriations Committee.

SB 327 (Jackson, Ch. 886, Stats. 2018) requires manufacturers of connected devices to equip those devices with reasonable security features appropriate to the nature of the device.

AB 2167 (Chau, 2018) would have amended CMIA to include within the definition of "medical information" any information in possession of, or derived from, a digital health feedback system. This bill failed passage on the Senate Floor.

AB 658 (Calderon, Ch. 296, Stats. 2013) *See* Comment 3.

AB 1298 (Jones, Ch. 699, Stats. 2007) subjects any business organized to maintain medical information for purposes of making that information available to an individual or to a health care provider, as specified, to the provisions of CMIA.

PRIOR VOTES:

Given the recent gutting and amending of this bill, all previous votes are irrelevant.

****