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

AB 2089 (Bauer-Kahan)
Version: April 21, 2022
Hearing Date: June 21, 2022
Fiscal: Yes
Urgency: No
CK

SUBJECT

Privacy: mental health applications: mental health application information

DIGEST

This bill includes mental health application information in the definition of "medical information" and the businesses that offer those applications to consumers in the definition of a provider of health care for purposes of the Confidentiality of Medical Information Act (CMIA).

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 addresses mental health applications that collect mental health information and that are offered by businesses for the purpose of allowing individuals to manage their information or even for diagnosis, treatment, or management of a medical condition. The bill deems the application information as medical information and the businesses offering them as providers of health care, bringing them within the protective ambit of CMIA.

The bill is sponsored by the author and supported by various consumer and privacy groups, including ACLU California Action. There is no known opposition. 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 "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).)

8) 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 their 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).)

9) 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).)

10) 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).)

11) 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).)

12) 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 "mental health application" to mean a mobile-based application that collects mental health application information from a consumer, markets itself as facilitating mental health services to a consumer, and uses the information to facilitate mental health services to a consumer.

2) Defines "mental health application information" as information related to a consumer's inferred or diagnosed mental health or substance use disorder, as defined, collected by a mental health application.

3) Includes mental health application information in the definition of "medical information" in CMIA.

4) Provides that a business that offers a mental health application to a consumer for the purpose of allowing them 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.

5) Requires any business that offers a mental health application, when partnering with a provider of health care to provide mental health application services, to notify the provider of health care of all reportable data breaches and known violations of CMIA in the past three years before finalizing an agreement between the entities.

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

The COVID-19 pandemic has arguably fundamentally altered our society and the health care system. While there was already a trend toward Californians and health care professionals relying on digital health products and services, the pandemic has expedited the process.

One particular area this is occurring in is mental health care. The pandemic has only exacerbated individuals' mental health issues, and with social distancing in full effect, many have turned to mental health apps and online mental health services. The concern with such tools is that while mental health information collected by a heath professional would be considered "medical information" and covered by existing medical privacy laws, because this information is being collected by apps and websites, meaning at the patient level and outside of a medical facility, it will not necessarily be captured under the existing definition of medical information.

The results of a Consumer Reports investigation frames the issue well:

> Type "mental health" or a condition such as anxiety or depression into an app store search bar, and you can end up scrolling through endless screens of options. As a recent Consumer Reports investigation has found, these apps take widely varied approaches to helping people handle psychological challenges—and they are just as varied in how they handle the privacy of their users.
>
> These apps are particularly important tools these days. Four in 10 Americans reported experiencing depression or anxiety because of the pandemic, according to a nationally representative survey of 2,982 U.S. adults conducted by Consumer Reports in December.
>
> Mental health apps take a number of approaches to providing help. Some connect you with licensed therapists over video. Conversations with therapists are typically covered by the same state and federal health privacy rules that apply to in-person therapy or to any doctor's appointment.

> But the same apps or similar-sounding ones may provide guided meditations, mood-tracking diaries, therapy chatbots, and cognitive behavioral therapy exercises. Along the way, you might be asked to complete a questionnaire on your mental health symptoms.
>
> The data you provide as you use those features might not necessarily be treated as confidential by the app developers, or by the law.
>
> Researchers in Consumer Reports' Digital Lab evaluated seven of the most popular options, representing a range of approaches, to gain more insight into what happens to your personal information when you start using a mental health app. . . .
>
> In general, these mental health services acted like many other apps you might download. For instance, we spotted apps sharing unique IDs associated with individual smartphones that tech companies often use to track what people do across lots of apps. The information can be combined with other data for targeted advertising. Many apps do that, but should mental health apps act the same way? At a minimum, Consumer Reports' privacy experts think, users should be given a clearer explanation of what's going on.
>
> "Your mental health is incredibly personal," says Justin Brookman, director of privacy and technology policy at Consumer Reports. "You should be able to reach out for help without worrying about how that data might be shared or misused."[1]

Such findings create legitimate concerns about how this data is being protected and how it synchronizes with consumers' expectations. Mental health information is incredibly sensitive, amplifying the impact of poor data security and any resulting breaches and identity theft. Simply the collection and utilization of this information for targeted advertising can lead to emotional harms, heightened anxiety, and even impacts beyond that depending on who receives the information.

Legislation is arguably needed to strike an appropriate balance between broadened access to mental health information and services for the public good and protection of the fundamental right to privacy. Given the sensitivity of mental health information and the increasing collection of it outside the protective ambit of our medical confidentiality laws, this bills looks to expand CMIA to cover it. The bill includes within the definition of "medical information" "mental health application information." That term is defined

---

[1] Thomas Germain, *Mental Health Apps Aren't All As Private As You May Think* (March 2, 2021) Consumer Reports, https://www.consumerreports.org/health-privacy/mental-health-apps-and-user-privacy-a7415198244/ [as of June 9, 2022].

as information related to a consumer's inferred or diagnosed mental health or substance use disorder collected by a mental health application, which is a mobile-based application that collects mental health application information from a consumer, markets itself as facilitating mental health services to a consumer, and uses the information to facilitate mental health services to a consumer.

The bill also deems a business that offers such applications to a consumer for the specific purpose of allowing them to manage their information or to diagnose, treat, or manage a medical condition a provider of a health care and therefore subject to CMIA.

This inclusion creates guardrails that are arguably necessary to protect this privately-collected but particularly sensitive information that consumers likely expect to be kept confidential. 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.)

The bill also places an obligation on businesses that offer these mental health applications to notify other providers of health care that they partner with of all reportable data breaches as well as known violations of this bill in the preceding three years before finalizing an agreement between the entities.

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 mental health applications at issue here collect information directly from consumers, the information is arguably not "medical information," as defined in CMIA. To ensure the protective umbrella of CMIA covers this information, the bill makes clear that CMIA covers mental health applications that collect sensitive information from individuals, and makes businesses offer them providers of healthcare.

4. Stakeholder positions

According to the author:

> Apps and other digital services that provide mental healthcare use predatory advertising and misleading privacy standards to create a false sense of security for consumers. When Californians are at their most vulnerable point, they must know their information is safe and their health information is private and secure. This bill finds a balance to protect consumer's information in a uniquely sensitive and vulnerable to exploitation.

Writing in support, ACLU California Action argues:

> Current privacy laws do not adequately protect the sensitive information collected by mental healthcare apps. In California, patient privacy is protected by the Confidentiality of Medical Information Act (CMIA) and the Health Insurance Portability and Accountability Act of 1996 (HIPAA), neither of which contemplate personal health information generated by technology outside the traditional care setting. 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 technologies, such as mental health apps, do not fall cleanly into this rubric. . . .
>
> This highly sensitive data is shared without consumer knowledge, especially because consumers often assume their information is protected

> under medical privacy laws. Information people thought was going to be used to provide them care was going to advertisers and other third parties. BetterHelp, Sanity & Self, Talkspace, and Wysa apps have all been sending data to Facebook, for example.
>
> AB 2089 is necessary to provide users with the medical privacy protections many wrongly assume mental health app data already has and to ensure the information provided to improve mental wellbeing is not used against the user.

ATA Action writes in a support if amended position. It states that it believes the changes made by the bill "will make it easier for telehealth providers to deliver high-quality, affordable health care services to California patients without being burdened with overly restrictive data privacy provisions" but seeks amendments to narrow the scope of the bill.

SUPPORT

ACLU California Action
County Behavioral Health Director's Association of California
Depression and Bipolar Support Alliance
Electronic Frontier Foundation
Steinberg Institute

OPPOSITION

None known

RELATED LEGISLATION

Pending Legislation: SB 1184 (Cortese, 2022) authorizes a provider of health care or a health care service plan to disclose medical information to a school-linked services coordinator pursuant to a written authorization. This bill is currently pending referral in the Assembly.

Prior Legislation:

AB 1436 (Chau, 2021) would have prohibited a business that offers a "personal health record system" from knowingly using or disclosing the "personal health record information" of a person without first obtaining a signed authorization, as specified. This bill died in the Senate Appropriations Committee.

AB 1252 (Chau, 2021) would have revised CMIA to define personal health record (PHR) and personal health record information (PHRI), and deem a business that offers PHR

software or hardware to a consumer, as specified, for purposes of allowing the individual to manage their information, or for the diagnosis, treatment, or management of a medical condition of the individual, to be a "health care provider" subject to the requirements of CMIA. This bill died on the Assembly Floor.

AB 2280 (Chau, 2020) was substantially similar 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) required 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) subjected 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:

Assembly Floor (Ayes 70, Noes 1)
Assembly Appropriations Committee (Ayes 13, Noes 0)
Assembly Privacy and Consumer Protection Committee (Ayes 10, Noes 0)
Assembly Health Committee (Ayes 12, Noes 1)

****