Date of Hearing: April 22, 2021

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Ed Chau, Chair
AB 1252 (Chau) – As Amended April 13, 2021

SUBJECT: Information privacy: digital health feedback systems

SUMMARY: This bill would revise the Confidentiality of Medical Information Act (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 the CMIA. Specifically, **this bill would**:

1) Provide that any business that offers PHR software or hardware to a consumer, including a mobile application or other related device that is designed to maintain PHRI, as defined, 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, to be a provider of health care, as specified.

2) Define the following:

   - "PHR" to mean a commercial internet website, online service, or product that is used by an individual and that collects the individual's PHRI.

   - "PHRI" to mean individually identifiable information, in electronic or physical form, about an individual's mental or physical condition that is collected by a PHR 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 PHR.

3) Make other technical and conforming changes.

EXISTING LAW:

1) Specifies, under the federal Health Insurance Portability and Accountability Act (HIPAA), privacy protections for patients' protected health information and generally provides that a covered entity, as defined (health plan, health care provider, and health care clearing house), may not use or disclose protected health information except as specified or as authorized by the patient in writing. (45 C.F.R. Sec. 164.500 et seq.)

2) Provides, under the California Constitution, that all people have inalienable rights, including the right to pursue and obtain privacy. (Cal. Const. art. I, sec. 1.)

3) Prohibits, under CMIA, 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 Sec. 56 et seq.)

4) Defines "medical information" 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. CMIA defines "individually identifiable" to mean 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 Sec. 56.05(g).)

5) 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 of treatment of the individual, shall be deemed to be a provider of health care subject to the requirements of the CMIA. (Civ. Code Sec. 56.06(a).)

6) Provides that any provider of health care, 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 Sec. 56.36.)

7) Establishes the California Consumer Privacy Act of 2018 (CCPA) and provides various rights to consumers pursuant to the act. Subject to various general exemptions, a consumer has, among other things:

   - the right to know what PI a business collects about consumers, as specified, including the categories of third parties with whom the business shares PI;

   - the right to know what PI a business sells about consumers, as specified, including the categories of PI that the business sold about the consumer and the categories of third parties to whom the PI was sold, by category or categories of PI for each third party to whom the PI was sold;

   - the right to access the specific pieces of information a business has collected about the consumer;

   - the right to delete information that a business has collected from the consumer;

   - the right to opt-out of the sale of the consumer's PI if over 16 years of age, and the right to opt-in, as specified if the consumer is a minor; and the right to equal service and price, despite exercising any of these rights. (Civ. Code Sec. 1798.100 et seq.)

8) Generally requires under the CCPA that a business subject to the CCPA do all of the following, among other things: comply with the above requirements, provide various notices to those ends, and execute various requests upon receipt of a verifiable consumer request, as specified; and provide certain mechanisms for consumers to make their lawful requests,

including a clear and conspicuous link titled "Do Not Sell My Personal Information" on the business's internet homepage to enable consumers, or a person authorized by the consumer, to opt-out of the sale of the consumer's PI. (Civ. Code Sec. 1798.100 et seq.)

9) Prohibits a third party from selling PI about a consumer that has been sold to the third party by a business unless the consumer has received explicit notice and is provided an opportunity to exercise the right to opt-out as specified. (Civ. Code Sec. 1798.110(d).)

10) Provides various exemptions under the CCPA, including for, among other things medical information and health care providers governed by the Confidentiality of Medical Information Act (CMIA) (Civ. Code Sec. 56 et seq.), and providers of health care and protected health information that is collected by a covered entity or business associate governed by the HIPAA, as specified. (Civ. Code Sec. 1798.145(c).)

FISCAL EFFECT: Unknown

COMMENTS:

1) **Purpose of the bill**: This bill seeks to ensure that commercial websites and applications that collect consumer health data are subjected to California's medical privacy laws. This bill is author sponsored.

2) **Author's statement**: 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. The author states that 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 combine ingestible microchip sensors with pharmaceuticals and communicate with a "patch" that 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.

   According to the author, appropriate guardrails are necessary to protect privately-collected information in line with the patient's or consumers reasonable expectation of privacy. The author argues that this bill 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.

3) **State and federal medical privacy laws**: 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 (PHI) is any information held by a covered entity which concerns health status, provision of health care, or payment for health care that can be connected to an individual. HIPAA privacy regulations require health care

providers and organizations to develop and follow procedures that ensure the confidentiality and security of PHI when it is transferred, received, handled, or shared. HIPAA further requires reasonable efforts when using, disclosing, or requesting PHI, to limit disclosure of that information to the minimum amount necessary to accomplish the intended purpose.

California's CMIA also protects medical information and restricts its disclosure by health care providers, and health care service plans, as specified. Under existing law, a corporation organized for the purpose of maintaining medical information in order to make that information available to the patient, or a provider at the request of the patient for purposes of diagnosis or treatment, is deemed to be a "provider of health care" subject to the requirements of the CMIA. AB 658 (Calderon, Ch. 296, Stats. 2013) further ensured 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 or for the diagnosis, treatment, or management of a medical condition of the individual, is also subject to the CMIA. While the chaptered version of AB 658 had no recorded opposition, the Chamber of Commerce opposed an earlier version of that bill because it was "unclear which mobile application software providers [would] be included. There are many small companies offering a variety of mobile apps that may be captured in the bill. For instance, it is difficult to determine if an app used for health fitness would be captured." To address those concerns, the author of AB 658 accepted amendments in the Assembly Judiciary Committee which clarified that the provisions of the bill would apply only to medical information, as defined by the CMIA, meaning information which originates with a covered entity.

Subsequently, the Legislature considered AB 2688 (Gordon, 2016) which sought to regulate the disclosure of information in possession of or derived from a commercial health monitoring program to a third party without providing clear and conspicuous notice and obtaining the consumer's affirmative consent. The introduced version of that bill would have expanded the CMIA to cover commercial health information devices (such as the "FitBit"), but was amended on March 28, 2016 to separate its provisions from CMIA and shift those requirements to a separate chapter in the Business and Professions Code. When AB 2688 ultimately died on the Senate floor, privacy advocates were in opposition because the bill did not create strong enough protections for privacy, whereas a coalition of technology companies were also in opposition because the bill in its current form would result in "unintended consequences, logistical difficulties, and consumer harm."

As with the bills noted above, the Legislature must once again consider the question of whether health and medical information are adequately protected by existing privacy laws. Despite the sensitive nature of information collected by mobile medical and health applications, medical information and PHI generally only receive such a classification when it *originates* with a health care provider or other covered entity. As noted in a recent law review article, despite HIPAA and CMIA protecting health information in the hands of health care professionals and health care institutions, these laws do not apply to user-generated data from medical apps, nor do they apply to information that is not traditionally considered health information (such as geolocation or gait) that could be used to discriminate against a person because of an association with a medical condition.[1]

---

[1] Andrews, *A New Privacy Paradigm in the Age of Apps* (2018) 53 Wake Forest L. Rev. 422

Accordingly, this bill would designate any business that offers PHR software or hardware to a consumer as a "provider of healthcare" under CMIA, thus determining that the manufacturers, operators, and developers of the digital pill software and hardware that collect and send health data cannot sell or disclose an individual's information without prior authorization. Notably, the Legislature enacted the CCPA (AB 375, Chau, Ch. 55, Stats. 2018), which gives consumers certain rights regarding their PI, including: (1) the right to know what PI that is collected and sold about them; (2) the right to request the categories and specific pieces of PI the business collects about them; and (3) the right to opt out of the sale of their PI, or opt-in in the case of minors under16 years of age. Largely due to the necessary information sharing in the healthcare setting and the protections found in CMIA and HIPAA, medical information and protected health information, as defined in those bodies of law, are exempt from the CCPA. Similarly, providers of health care under CMIA and covered entities under HIPAA are exempt from the CCPA. Staff notes that due to the nature of the information generated by digital health feedback systems, and the fact that they are used in conjunction with a prescription while the patient is under the care of a doctor, CMIA is likely a better governing scheme than the CCPA for this information, in that CMIA allows information sharing amongst healthcare providers, thereby facilitating better healthcare.

4) **Similar legislation has been approved by this Committee in the past**: Two years ago, this Committee passed AB 2167 (Chau, 2018), which was substantially similar to this bill. AB 2167 received opposition in the Senate from the Advanced Medical Technology Association (AdvaMed) and the California Life Sciences Association who argued that it would have prematurely regulated digital health feedback systems and impose significant compliance and legal costs. Specifically, the opposition argued:

> The additional liability under the California Medical Information Act is unnecessary and overly burdensome given the substantial bodies of applicable regulations and guidance, both federal and private, at the national level (international standards are also important), all of which have been closely followed by innovators in this space. It is important to note that use of this technology requires willing and knowing participation from the patient – the technology will not work unless used correctly and the patient maintains ownership and control of any data that is generated.

This year, the same two groups are in opposition, and argue that "AB 1252 would increase compliance, legal and other administrative costs, while discouraging investment in this beneficial technology, without evidence of a well-documented problem in the already heavily regulated space of connected medical technology. This bill could therefore be a solution in search of a problem and creating unintended consequences for emerging technologies that could help to dramatically improve patient care." (Emphasis added)

Staff notes that by the opposition's own admission, these apps are being used in patient care, and not solely by consumers.

The opposition further notes that "existing privacy laws, and FTC section 5 unfair and deceptive business practices laws, create sweeping powers to regulate in this area where business practices diverge from statements or claims made to the patient. The FDA and FTC have for years maintained a MOU to facilitate enforcement over medical technology and the combined force of the regulators is more than sufficient to protect this form of information."

Staff notes that while the power to address unfair or deceptive trade practices is indeed broad, the FTC has generally only chosen to take action when an application developer fails to disclose in advance that it will be invading a person's privacy. In other words, if an application developer states in advance that it will be collecting and sharing a person's information, the FTC will generally not argue that the developer misrepresented its practices.

On this point, research shows that these privacy related-issues extend beyond digital health feedback systems and are endemic to digital medicine itself. "People care deeply about the privacy of the information collected by their medical apps. Yet our studies show that information from medical apps is collected directly and indirectly and then shared with marketers and other third parties in ways which can harm the app user. Vast in scope and packaged with information not traditionally thought of as implicating health, information from medical apps is sold to third parties including employers and insurers. In one instance, an insurer bought health-related digital data from about three million people from a data aggregator. […] Existing laws do not sufficiently protect the privacy of medical app users. An alternative approach is necessary that recognizes the unique challenges raised by medical apps in terms of the scope of information they collect, the nature of that information, and the context in which it is collected."

This bill, which would extend the existing CMIA framework of consent prior to disclosure of personal information to the data collected by digital health feedback systems, would hold digital health feedback system creators and operators to the same high standards as healthcare providers, while still allowing for the necessary sharing of information for patient health care. A coalition of industry groups, including the California Chamber of Commerce, Internet Association, Silicon Valley Leadership Group, and the California Manufacturers & Technology Association (Chamber coalition) argue in opposition:

> AB 1252 is overbroad, turning commonplace fitness trackers, basic household devices, and social media websites into medical devices. AB 1252 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 […] 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.

Staff notes that the structure of this bill is not unprecedented. In fact, it was modeled after AB 658 (Calderon, Ch. 296, Stats. 2013) which applied CMIA to any business that offers

software or hardware to consumers, including a mobile application or other related device that is designed to maintain medical information to allow an individual to manage his or her information, or for the diagnosis, treatment, or management of a medical condition of the individual. Further, the types of applications and websites noted by the Chamber coalition (*e.g.,* digital scales, fitness wearables, blood sugar monitors, thermometers, fitness tracking tools, wearable fitness devices, or website where individuals can post information about their mental condition, such as an online happiness/mood diary) in their argument that this bill is "too broad," appear to be the exact type of commercial applications the author intends to capture with this bill.

In fact, without AB 1252, commercial entities offering these apps would be able to use an individual's health information, such as blood sugar levels, fertility cycle, or emotional state, to target advertising to them, which seems inappropriately manipulative given the sensitivity of the information. In support of this bill, Oakland Privacy notes that CMIA is a long-established statutory scheme which should give manufacturers of PHRs a substantial amount of certainty. Oakland Privacy writes that AB 1252 addresses a loophole in privacy protections that has occurred from rapid technological innovation:

> Long-standing medical records protections do not include and did not envision such apps and websites holding personal and private medical information, and consumers being instructed to use them by their medical providers. Similarly, recently enacted sweeping privacy protections in the California Consumer Privacy Act of 2018 exempted medical-related information due to longstanding regulatory protocols for medical records.
>
> This left services like "digital pills" or wife-enabled blood sugar measuring devices in a space regulated by neither, but still presenting health privacy concerns that should not be ignored.
>
> Assembly Bill 1252 addresses this gap by expanding the scope of existing health privacy law, the Confidentiality of Medical Information Act (CMIA) to cover such devices, applications and websites. By using existing and well-established protocols to cover the gap, Assembly Bill 1252 provides a well-understood and tested framework to encompass new technologies without creating a brand new regulatory structure. This is a sound approach and
> should ease implementation complexity for providers newly subject to the law."

Additionally, a coalition of consumer advocacy and privacy groups including the ACLU of California, counter the Chamber coalition's arguments and write in support:

> In California, patient privacy is protected by the […] 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 would help protect sensitive information generated by new forms of health technology, aligning privacy rights around data collected in new ways with all other medical information, and would also require that manufacturers apply appropriate data security standards. 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. For these reasons and many others, we support this bill. (Emphasis in original.)

5) **Prior legislation**: AB 2280 (Chau, 2020) was identical to this bill. The bill was held in the Senate Judiciary Committee.

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 the Confidentiality of Medical Information Act (CMIA) applies to information derived from or in the possession of these systems. AB 384 was held on the Senate Appropriations Committee Suspense File.

AB 2167 (Chau, 2018) *See* Comment 4.

AB 2747 (Assembly Committee on Judiciary, Ch. 913, Stats. 2014) extends CMIA provisions to 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.

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

AB 1298 (Snyder, 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 the Confidentiality of Medical Information Act (CMIA).

6) **Double referral**: This bill was double-referred to the Assembly Committee on Health, where it was heard on March 23, 2021 and passed on a 11-2 vote.

REGISTERED SUPPORT / OPPOSITION:

Support

American Civil Liberties of California

Consumer Reports
Electronic Frontier Foundation
National Association of Social Workers, California Chapter
Oakland Privacy
Privacy Rights Clearinghouse

Opposition

Advanced Medical Technology Association (ADVAMED)
California Chamber of Commerce
California Life Sciences Association
California Manufactures & Technology Association
Civil Justice Association of California
Entertainment Software Association
Insights Association
Internet Association; the
Masimo Corporation
National Payroll Reporting Consortium
Silicon Valley Leadership Group
State Privacy and Security Coalition, INC.
Technet

Analysis Prepared by: Nichole Rocha / P. & C.P. / (916) 319-2200