Date of Hearing: April 23, 2019

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Ed Chau, Chair
AB 384 (Chau) – As Introduced February 5, 2019

SUBJECT: Information privacy: digital health feedback systems

SUMMARY: This bill would define "medical information" for purposes of the Confidentiality of Medical Information Act (CMIA) to include any individually identifiable information in the possession of or derived from a digital health feedback system, as specified. The bill would also require a manufacturer that sells or offers to sell a digital health feedback system to a consumer in California to equip the system with reasonable security features. Specifically, **this bill would**:

1) Define "digital health feedback system" to mean an ingestible sensor that collects and sends information about an individual that may be used in conjunction with either of the following:

    - A sensor or device placed inside or worn on the body that collects and sends information about an individual.

    - A software platform that is connected to the internet, directly or indirectly, or to another device that receives and displays information collected or sent from a sensor or device as described in the paragraph above.

2) Include within the definition of "medical information" in the CMIA "any individually identifiable information in electronic or physical form, in possession of or derived from, a digital health feedback system."

3) Require any manufacturer or operator that sells or offers to sell a digital health feedback system to a consumer in California to equip the device or software application, and the system, with reasonable security features appropriate to the nature of the device, software application, or system, and the information it may collect, contain, or transmit, and require the features to protect the system and any information contained therein from unauthorized access, destruction, use, modification, or disclosure.

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.)

FISCAL EFFECT: Unknown

COMMENTS:

1) **Purpose of the bill**: This bill seeks to implement reasonable regulations for the use of "digital pills" by defining "digital health feedback systems," amending the definition of "medical information" in the CMIA, and requiring that manufacturers and operators equip digital health feedback systems with reasonable security features appropriate to protect the system and any information contained therein. This is an author-sponsored bill.

2) **Author's statement**: According to the author, "[w]hile technology stands to improve how healthcare is delivered, these advancements do not come without risk. Health and medical information is, by its very nature, deeply personal and sensitive. New technology makes medical information easily and quickly accessible via apps and websites, and California has ensured that medical information held by mobile devices is protected under our privacy laws. However, in order to be considered 'medical information,' this information generally needs to be generated by a healthcare provider. Information generated by a digital health feedback system, meaning at the patient level and outside of a medical facility, is not necessarily captured under the existing definition of medical information. However, information about whether a patient took their medication and how that medication interacted in their body is unquestionably of a medical nature. Therefore, it is imperative that the information generated by digital health feedback systems is classified as medical information, and developers and operators of hardware, software, and applications are prohibited from sharing this information and data without the patient's informed consent."

3) **Digital medicine**: Technology enables individuals to receive more detailed and time-sensitive information about the world around them all the time. A network of devices with the ability to connect to the internet (commonly known as "the Internet of Things" or IOT)

has created previously unimagined conveniences for consumers who have come to rely on connected devices such as cellphones, fitness applications, smart appliances, smart cars, and wearable devices.

The global digital health market has grown exponentially in the past five years, fueled by IoT development, increased mobile device adoption, and big data investment. (Chamberlin & Gretz, *Internet of Things: Small IoT Projects Pay the Way for Future Transformation*, BLUEMINE: HORRIZONWATCH (Mar. 6, 2016).) Historically, the medical device industry focused on implants and direct therapies, but new medical technologies also leverage connectivity and data aggregation, necessitating enhanced privacy protections to protect patients and/or consumers.

Research shows that a significant number of Americans depend on medical applications as part of their medical care, with the majority of smartphone users having downloaded a health application. (Krebs & Duncan, *Health App Use Among US Mobile Phone Owners: A National Survey*, 3 JMIR mHealth and UHealth 1, 5 (2015).) As of July 2018, Google Play had over 40,000 applications in the medical category and nearly 75,000 in the health and fitness category. These applications can collect an extraordinary amount of information, including a user's sleep schedule, medication information, blood pressure, cholesterol level, menstrual cycle, blood oxygen level, and location.

Relevant to this bill, several forms of "digital pills" that send information from places like the digestive tract or bloodstream to an application have recently been developed, with a few already in use. These digital pills, which combine ingestible microchip sensors with pharmaceuticals and patches worn by the patient, can record whether, when, where and in what quantity a drug is released, as well as information about the physical state of the person taking the drug, such as temperature, activity level, heart rate, and respiration. Digital pills then transmit signals and information about the patient to devices like mobile phones, tablets, and computers belonging to the patient, the patient's caregivers, or the patient's doctor. (Avery & Liu, *Bringing Smart Pills to Market: FDA Regulation of Ingestible Drug/Device Combination Products*, 66 Food & Drug L.J. 329, 330-32 (2011).)

These pills and their accompanying technology stand to provide information that may drastically improve the lives of many people. For example, an estimated 50 % of patients with chronic diseases in developed countries do not take their medication, as prescribed. This can cause relapse and recurrence of chronic disease and results in an estimated $100 billion - $300 billion in avoidable healthcare costs. (Whitefield, Bus. Wire *US FDA Accepts Digital Medicine Drug Application for Otsuka and Proteus Digital Health*, (Sept. 10, 2015), found at < https://www.businesswire.com/news/home/20150910005497/en/ U.S.-FDA-Accepts-Digital-Medicine-Drug-Application > [as of Mar. 18, 2019].) By measuring medication adherence, digital health feedback systems could allow healthcare professionals to more effectively tailor treatment of chronic diseases to individual patients, which could both lead to better health outcomes and save billions of dollars in healthcare costs. (*Id*.)

Yet, despite digital health feedback systems' potential for positive impact, there are significant concerns related to privacy and data security, which may act as barriers to their success. Specifically, should privacy laws proactively determine how information generated and collected by these systems is disclosed, and to whom? Furthermore, are current privacy and data collection laws sufficient to ensure that data created and transmitted via digital

health feedback systems is secure? Consumer Reports, in support, argues that this bill is necessary because innovative medical technology was not contemplated when current laws were put in place. Consumer Reports writes in support:

> In California, patient privacy is protected by the Confidentiality of Medical Information Act (CMIA)2 and the Health Insurance Portability and Accountability Act of 1996 (HIPAA)3. 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 digital health feedback systems do not fall into this rubric. […]
>
> AB 384 would protect sensitive information generated and collected by digital feedback systems by expanding the definition of "medical information" under CMIA to include this new way of generating data. If enacted, this bill would align privacy rights around data collected by digital pills with all other medical information, and would also require that manufacturers apply appropriate data security standards to digital pills. These added protections would add certainty for patients that using smart pills will not jeopardize their privacy and potentially impact them in other areas of their lives. It is critical that AB 384 be put in place as the marketplace for this type of medical technology expands and becomes a prevalent feature of healthcare.

4) **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, and now by digital pills, 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. (Andrews, *A New Privacy Paradigm in the Age of Apps* (2018) 53 Wake Forest L. Rev. 422 (hereinafter, Andrews).)

Additionally, despite California law seemingly protected by applications designed for purposes of allowing the individual to manage their information, or for the diagnosis, treatment, or management of a medical condition, the law only protects *medical information* (meaning it must be generated in a traditional healthcare setting), and the statute explicitly states that other protections of confidentiality in the physician-patient relationship do not apply. (*See* Civ. Code Sec. 56.06(b) and (c).)

Accordingly, this bill would proactively designate information generated by digital health feedback systems as medical information, thus determining, at least for the purposes of California's CMIA, 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, last year, 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.

5) **Last year's digital pill legislation**: Last year 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, but argue that they are already subject to CMIA's confidentiality and non-disclosure provisions. "The additional liability under the California Medical Information Act (CMIA) is unnecessary and overly burdensome for two key threshold reasons. First, the CMIA already covers the core activities ostensibly targeted by AB 384. Currently, the CMIA deems any business that offers software or hardware to consumers, including a mobile application or other related device designed to maintain medical information, for purposes of allowing the individual to manage his information, or for the diagnosis, treatment, or management of a medical condition of the individual, to be a 'provider of health care' (Civil Code [sec.] 56.06(b)). This means such businesses, including those involved in digital health feedback systems, are already subject to the CMIA's confidentiality and nondisclosure requirements with respect to any individually identifiable patient medical information they access or maintain."

As noted above in Comment 4, CMIA does not necessary apply to medical or health information generated at the individual level, outside of a traditional healthcare setting. In fact, a strict reading of the relevant statute would allow an application developer or business that maintains the application data, to avoid liability under CMIA by simply claiming that they are providing information for entertainment purposes, rather than for medical or health purposes. It is also questionable, under this reasoning, whether information that may predict health status (such as gait information), that an individual is not using to assess their own health, but could be used by others to assess patient health, would be protected under the CMIA. (*See* Civ. Code Sec. 56.06(b).)

The opposition further notes that "the FTC through its Section 5 'unfair and deceptive business practices' enforcement authority has broad, sweeping powers to regulate in this area where business practices diverge from statements or claims made to the patient. As manufacturers already grant total control and ownership to the patient, if data were used in any other way, the manufacturer would be in violation of the Federal Trade Commission Act. The [Food and Drug Administration] FDA and FTC have for years maintained a memorandum of understanding (MOU) to facilitate enforcement over medical technology. Additionally, last year, the FDA announced an expansion of regulation into the digital health

space – we hope to see how this regulatory framework functions before imposing additional regulation at the state level that could conflict with or impose needless burdens on a new technology that has not shown deficiencies with respect to data stewardship."

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. (*See*, e.g., *PayPal Settles FTC Charges that Venmo Failed to Disclose Information to Consumers About the Ability to Transfer Funds and Privacy Settings; Violated Gramm-Leach-Bliley Act*, FTC (Feb. 27, 2018).)

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." (Andrews at p. 28.)

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. Staff notes that the author and the opposition have been working together in an effort to find common ground on these issues, and have discussed expanding the provisions of the bill to apply to digital medicine more broadly to ensure that the privacy of California residents is appropriately protected, while still ensuring that they can benefit from the advancements of digital medicine.

6) **Manufacturers that sell digital health feedback systems must equip systems with reasonable security features**: The health care industry is plagued with data breaches. (Snell, *How Much Do Healthcare Data Breaches Cost Organizations?* Health IT Security, (Feb. 2018) <https://healthitsecurity.com/news/how-much-do-healthcare-data-breaches-cost-organizations> [as of Mar. 18, 2019].) Each act of data transmission presents some risk that data will be breached, even with security precautions in place, and the frequency of breaches is increasing. In 2015, 113 million electronic health records were breached. (*See* Ponemon Inst., *Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data* (2016) (discussing "the increased frequency of [data] breaches" in the health care industry). At the same time, connected medical devices – components of the so-called IoT – are multiplying, opening more holes in security.

Digital health feedback systems stand to greatly improve adherence to prescriptions, and thus healthcare, as discussed in Comment 3, above. However, at the core of the system are digital applications and software, which are ripe for data security breach. Accordingly, this bill would require a manufacturer or operator that sells or offers to sell a digital health feedback system to a consumer in California equip the device or software application, and the system, with reasonable security features appropriate to the nature of the device, software application, or system, and the information it may collect, contain, or transmit, and require the features to protect the system and any information contained therein from unauthorized access, destruction, use, modification, or disclosure.

AdvaMed and the California Life Sciences Association additionally argue in opposition that requiring "reasonable security features" would create persistent questions of liability for the industry.

> [A] thoroughly comprehensive regulatory and policy frameworks exist at both the national and international levels, and these frameworks are continuing to evolve in important ways. These substantial bodies of applicable regulations, guidance, and standards, both federal and private at consequences for doing so would be significant (e.g., a barrier to entry for certain markets and costly redesigns of technology, among many other things). 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.

Staff notes that this requirement is consistent with other proposals that the Legislature has reviewed in the past few years. (*See*, e.g., AB 658 (Calderon, Ch. 296, Stats. 2013) and AB 1298 (Snyder, Ch. 699, Stats. 2007).) This language was crafted last year after some groups connected with the pharmaceutical industry expressed concern that the digital sensor component of the digital health feedback system which they are responsible for, cannot be "equipped" with reasonable security features as required by this bill. Indeed, the only sensor approved currently by the FDA is "a silicon chip about the size of a sand particle. With no battery or sensor, it is powered by the body itself. The chip contains small amounts of copper and magnesium. After being ingested the chip will interact with digestive juices to produce a voltage that can be read from the surface of the skin through a detector patch, which then sends a signal via mobile phone to inform the doctor that the pill has been taken." (Murray, *No More Skipping Your Medicine—FDA Approves First Digital Pill,* Forbes (Aug. 9, 2012).)

In response to the concerns raised by the opposition, the author writes:

> It is important to remember that while technology stands to improve how healthcare is delivered, these advancements do not come without risk. Information that is generated by a digital health feedback system, meaning at the patient level and outside of a medical facility, will not necessarily be captured under the existing definition of medical information. But information about whether a patient took his or her medication and how that medication interacted in his or her body is unquestionably of a medical nature. Therefore it is imperative that the information generated by digital health feedback systems is classified as medical information, and developers and operators of hardware, software, and applications are prohibited from sharing this information and data without the patient's informed consent.

Further, California cannot control federal regulations. As a Legislature, we often go beyond what the federal government requires or is willing to offer to individuals whose rights have been violated. The world of medical technology should be no different. That the opposition claims this field is regulated by federal "guidance" should not stop California from protecting the privacy of its residents. It is entirely within our purview to codify best practices in an industry to ensure all actors in a field are acting with due care.

7) **Prior legislation**: AB 2167 (Chau, 2018) was substantially similar to this bill. AB 2167 died on the Senate floor.

AB 375 (Chau, Ch. 55, Stats. 2018) *See* Comment 4.

AB 2935 (Chau, 2018) would prohibit the operator of a commercial health monitoring program from intentionally sharing or disclosing a consumers individually identifiable health monitoring information to or with a third party without first obtaining the consumers consent.

AB 2688 (Gordon, 2016) *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 4.

AB 1298 (Snyder, 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.

8) **Double-referral**: This bill was double-referred to the Assembly Committee on Health, where it was heard on March 26, 2019, and passed on a 10 - 3 vote.

REGISTERED SUPPORT / OPPOSITION:

Support

Consumer Reports

Opposition

Advanced Medical Technology Association
California Life Sciences Association

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