**SENATE JUDICIARY COMMITTEE**
**Senator Thomas Umberg, Chair**
**2023-2024 Regular Session**

AB 254 (Bauer-Kahan)
Version: April 17, 2023
Hearing Date: June 13, 2023
Fiscal: Yes
Urgency: No
CK

## SUBJECT

Confidentiality of Medical Information Act: reproductive or sexual health application information

## DIGEST

This bill includes "reproductive or sexual health application information" in the definition of "medical information" and the businesses that offer reproductive or sexual health digital services 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. Given the increasingly hostile environment around reproductive and gender-affirming healthcare, this bill addresses digital services that collect reproductive or sexual health information from consumers and that are offered by businesses for the purpose of allowing individuals to manage that 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 author-sponsored 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) Holds that the state constitution's express right to privacy extends to an individual's decision about whether or not to have an abortion. *(People v. Belous* (1969) 71 Cal.2d 954.*)*

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

4) 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.)

5) 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.)

6) 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(l).)

7) 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 health application information, 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(i).)

8) 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(o).)

9) 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).)

10) 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).)

11) 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).)

12) Provides that any business that offers a mental health digital service to a consumer for the purpose of allowing the individual to manage the individual's 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(d).)

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(e)-(f).)

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.)

15) Establishes the Reproductive Privacy Act, which provides that the Legislature finds and declares that every individual possesses a fundamental right of privacy with respect to personal reproductive decisions and, therefore, it is the public policy of the State of California that:
    a) every individual has the fundamental right to choose or refuse birth control; and
    b) every individual has the fundamental right to choose to bear a child or to choose to obtain an abortion, with specified limited exceptions.

16) Specifies, under the Insurance Information and Privacy Protection Act, requirements insurers must take to protect the confidentiality of an insured's medical information. (Ins. Code § 791.29 et. seq.)
    a) Requires a health insurer to recognize the right of a protected individual to exclusively exercise rights regarding medical information related to sensitive services that the protected individual has received, including reproductive health services. (Ins. Code § 791.29 (a)(2).)
    b) Prohibits a health insurer from disclosing medical information about sensitive health care services provided to a protected individual to the policyholder or any insureds other than the protected individual receiving care, absent written authorization of the protected individual receiving care. (*Id*. (a)(4).)

This bill:

1) Defines "reproductive or sexual health digital service" as a mobile-based application or internet website that collects reproductive or sexual health application information from a consumer, markets itself as facilitating reproductive or sexual health services to a consumer, and uses the information to facilitate reproductive or sexual health services to a consumer.

2) Defines "reproductive or sexual health application information" as information about a consumer's reproductive health, menstrual cycle, fertility, pregnancy, miscarriage, pregnancy termination, plans to conceive, or type of sexual activity collected by a reproductive or sexual health digital service, including, but not limited to, information from which one can infer someone's pregnancy status, menstrual cycle, fertility, hormone levels, birth control use, sexual activity, or gender identity.

3) Includes reproductive or sexual health application information in the definition of "medical information" in CMIA.

4) Provides that a business that offers a reproductive or sexual health digital service to a consumer for the purpose of allowing the individual to manage the individual's 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.

## 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 seek 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 reproductive or sexual health application 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 reproductive health care. The concern with such tools is that while reproductive, or sexual 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:

> If you use an app to track your menstrual cycle, you may enjoy the sometimes spot-on predictions about when your next period is coming. But your period-tracking app doesn't just offer insight. It gathers a lot of data about you along the way, too—maybe even more than you know.
>
> Period tracker apps collect deeply personal information that can include how often you have sex, whether you are trying to have a baby, if you get pregnant, and if you experience a miscarriage. When Consumer Reports last evaluated period tracker apps in 2020, our Digital Lab, which tests how well products and services protect consumers' privacy, found that the five apps we evaluated—which all store users' data in the cloud—provided no guarantee that this information would not be shared with third parties, even when users thought they were anonymous.
>
> These lax privacy protections have long been a concern because users' data can be used to target them with ads or even possibly to determine life insurance coverage or loan interest rates. Now that the Supreme Court has overturned Roe v. Wade—ending the constitutional right to an abortion—many app users may be newly worried that data about their fertility, missed periods, and more could be used against them in criminal and civil proceedings as circumstantial evidence that they've had an abortion. Some people who have miscarriages could also be implicated, because "miscarriages are often conflated with induced abortions in the . . . law," according to the Kaiser Family Foundation, and even insurers sometimes

> code them as such. These privacy concerns are set against the backdrop of newly restrictive abortion laws in many states.[1]

Such findings create legitimate concerns about how this data is being protected and how it synchronizes with consumers' expectations. Reproductive 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.

As stated, this all occurs in a frightening climate for reproductive rights. *Roe v. Wade* (1973) 410 U.S. 113, was the landmark U.S. Supreme Court decision that held the implied constitutional right to privacy extended to a person's decision whether to terminate a pregnancy, while allowing that some state regulation of abortion access could be permissible. *Roe* has been one of the most debated U.S. Supreme Court decisions and its application and validity have been challenged numerous times, but its fundamental holding had continuously been upheld by the Court until June 2022. On June 24, 2022, the Court published its official opinion in *Dobbs* and voted 6-3 to overturn the holding in *Roe*.[2] The majority opinion upholds the Mississippi law finding that, contrary to almost 50 years of precedent, there is no fundamental constitutional right to have an abortion. The opinion further provides that states should be allowed to decide how to regulate abortion and that a strong presumption of validity should be afforded to those state laws.[3]

The *Roe* decision was the foundation for allowing people the ability to control their reproductive lives because it established a federal constitutional right for anyone who could become pregnant in the United States to decide when and if to have children and prevented the criminalization of having an abortion or providing an abortion. Prior to *Roe*, legal abortion did exist in some states, but the choices available to those seeking to terminate an unwanted pregnancy were limited and disproportionately affected those who were younger, lower income, and members of communities of color.[4] In the wake of the *Dobbs* decision, it is very probable that abortion will be banned or severely

---

[1] Catherine Roberts, *These Period Tracker Apps Say They Put Privacy First. Here's What We Found* (May 25, 2022) Consumer Reports, https://www.consumerreports.org/health-privacy/period-tracker-apps-privacy-a2278134145/#:~:text=Overall%2C%20we%20recommend%20three%20of,researcher%20in%20CR's%20Digital%20Lab. All internet citations are current as of June 9, 2023.
[2] *Dobbs v. Jackson Women's Health* (2022) 597 U.S. _ (142 S.Ct. 2228) at p. 5, https://www.supremecourt.gov/opinions/21pdf/19-1392_6j37.pdf.
[3] *Id*. at 77.
[4] Rachel Benson Gold, *Lessons from Before Roe: Will Past be Prologue*, Guttmacher Institute (Mar. 1, 2003), https://www.guttmacher.org/gpr/2003/03/lessons-roe-will-past-be-prologue.

restricted in dozens of states,[5] with 13 states already having total abortion bans in effect.[6] Almost one-third of women and people who can become pregnant of reproductive age in the United States live in a state where abortion is not legal or is severely restricted.[7] If all the states expected to enact a total ban on abortion actually do, the number of patients who would find that their nearest clinic is in California could increase to 1.4 million, an almost 3,000 percent increase.[8] These increased attacks on reproductive freedom in this country only make the privacy concerns regarding reproductive health information all the more urgent.

In addition, as California and other states have implemented policies to ensure that transgender individuals are not discriminated against and can obtain gender-affirming care, other states have targeted transgender individuals and providers of gender-affirming care. According to Human Rights Watch, as of March 2022, legislatures nationwide had introduced over 300 anti-LGBTQ+ bills, over 130 of which specifically targeted transgender people.[9] Many states have been enacting statutes that potentially impose civil and criminal liability for providing to a minor, or helping a minor obtain, gender-affirming care. For example, Alabama recently enacted a bill that makes it a felony to provide, or help to provide, certain types of gender-affirming care.[10] Arkansas prohibits a physician or other healthcare provider from providing or referring certain types of gender-affirming care for a minor; a violation or "threatened violation" can be punished through a professional board or a civil action.[11] Thus, data collected by digital service providers online and through applications that may reveal one's gender identity, sexual activity, or their searches for gender-affirming care become increasingly sensitive as many corners of the country criminalize it.

---

[5] Elizabeth Nash and Isabel Guarnieri, *Six Months Post-Roe, 24 US States Have Banned Abortion or Are Likely to Do So: A Roundup*, Guttmacher Institute (Jan. 10, 2023) https://www.guttmacher.org/2023/01/six-months-post-roe-24-us-states-have-banned-abortion-or-are-likely-do-so-roundup.
[6] Sharon Bernstein, *Factbox: US. abortion restrictions mount after overturn of Roe v. Wade*, Reuters, (Oct. 4, 2022), available at https://www.reuters.com/business/healthcare-pharmaceuticals/us-abortion-restrictions-mount-after-overturn-roe-v-wade-2022-10-04/#:~:text=ACTIVE%20BANS,an%20abortion%20rights%20research%20group.
[7] Katie Shepherd, Rachel Roubein, and Caroline Kitchner, *1 in 3 American women have already lost abortion access. More restrictive laws are coming*, The Washington Post, (Aug. 22, 2022) https://www.washingtonpost.com/nation/2022/08/22/more-trigger-bans-loom-1-3-women-lose-most-abortion-access-post-roe/.
[8] April Dembosky, *As states ban abortion, Californians open their arms and wallets*, NPR (June 27, 2022), https://www.npr.org/sections/health-shots/2022/06/27/1103479722/as-states-ban-abortion-californians-open-their-arms-and-wallets.
[9] Human Rights Watch, Press Release, ICYMI: As Lawmakers Escalate Attacks on Transgender Youth Across the Country, Some GOP Leaders Stand Up for Transgender Youth (Mar. 24, 2022), https://www.hrc.org/press-releases/icymi-as-lawmakers-escalate-attacks-on-transgender-youth-across-the-country-some-gop-leaders-stand-up-for-transgender-youth.
[10] *See* Al. Code, § 26-26-4.
[11] Ark. Stats. §§ 20-9-1502 & 20-9-1504.

Legislation is arguably needed to strike an appropriate balance between broadened access to reproductive and sexual health information and services for the public good and protection of the fundamental right to privacy. Given the sensitivity of this 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" "reproductive or sexual health application information." That term is defined as information about a consumer's reproductive health, menstrual cycle, fertility, pregnancy, miscarriage, pregnancy termination, plans to conceive, or type of sexual activity collected by a reproductive or sexual health digital service, including, but not limited to, information from which one can infer someone's pregnancy status, menstrual cycle, fertility, hormone levels, birth control use, sexual activity, or gender identity.

The bill also deems a business that offers a reproductive or sexual health digital service to a consumer for the specific purpose of allowing them to manage the individual's information, or for the diagnosis, treatment, or management of a medical condition of the individual, a provider of 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.)

3. Building on previous legislation

This bill models several predecessor bills. AB 658 (Calderon, Ch. 296, Stats. 2013) 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."

Last year, AB 2089 (Bauer-Kahan, Ch. 690, Stats. 2022) provided similar protections to this bill but for mental health application information that related to a consumer's inferred or diagnosed mental health or substance use disorder.

4. Stakeholder positions

According to the author:

> Reproductive and sexual health information is clearly health information, and is particularly sensitive given the criminalization of almost any form of ending a pregnancy. Our current data protections do not speak to the sensitivity of this data. Apps and websites that explicitly market themselves as providing menstrual and pregnancy tracking are creating an expectation of healthcare and the associated privacy of information. Adding CMIA protections for these services is a critical and common sense step to ensure a sufficient baseline of privacy to protect consumers.

Writing in support, Oakland Privacy states:

> While it is empowering to have modern tools to get a better understanding of reproductive and sexual health, using these tools should not come at the expense of giving up privacy rights and being required to surrender sensitive health information. Furthermore, reproductive and sexual health digital products and service providers collect and share a lot of sensitive information and consumers don't know and often can't control who is accessing this data. Research has identified concerning practices with the collection, storage, selling and sharing of this sensitive reproductive and sexual health data. In addition, some entities have been found to use misleading privacy claims and predatory advertising

> practices. Consumers are left with a false sense of security that their data is private, safe and secure. AB 254 will give consumers an extra layer of protection and help with re-establishing trust in these digital services and products which is important now more than ever.

NARAL Pro-Choice California urges support for the bill: "At a time when reproductive health care is under threat this bill would urge businesses to take action to preserve reproductive freedom."

**SUPPORT**

accessnow
Accountable Tech
ACLU California Action
ADL
American Association of University Women – California
American Association of University Women – San Jose
American College of Obstetricians and Gynecologists District IX
California Legislative Women's Caucus
California Academy of Family Physicians
California Federation of Teachers
California Nurse Midwives Association (CNMA)
California Pan - Ethnic Health Network
Center for Digital Democracy
City and County of San Francisco Department on the Status of Women
Consumer Federation of America
Consumer Reports
Demand Progress
Doctors In Politics
EKO
Electronic Frontier Foundation
epic.org
Fairplay
Fight For The Future
Free Press
Friends of the Earth
glaad
Health Care Voices
Health Officers Association of California
KAIROS
Mozilla
NARAL Pro-Choice California
National Association of Social Workers, California Chapter
Oakland Privacy

She Persisted
Sister Song
Super-majority
ultraviolet Action
Vote Pro Choice

## OPPOSITION

None known

## RELATED LEGISLATION

Pending Legislation:

AB 352 (Bauer-Kahan, 2023) requires specified businesses that electronically store or maintain medical information on the provision of sensitive services, as specified, on or before July 1, 2024, to enable certain security features, including limiting user access privileges and segregating medical information related to sensitive services, as specified. It prohibits a health care provider, health care service plan, contractor, or employer from cooperating with any inquiry or investigation by, or from providing medical information to, an individual, agency, or department from another state or, to the extent permitted by federal law, to a federal law enforcement agency that would identify an individual or that is related to an individual seeking or obtaining an abortion or abortion-related services that are lawful under the laws of this state, unless authorized. AB 352 is currently pending referral in the Senate.

AB 793 (Bonta, 2023) prohibits a government entity from seeking or obtaining information from a reverse-location demand or a reverse-keyword demand, and prohibits any person or government entity from complying with a reverse-location demand or a reverse-keyword demand. AB 793 is currently pending referral in the Senate.

AB 1194 (Wendy Carrillo, 2023) amends the California Consumer Privacy Act to ensure that businesses comply with the obligations imposed by the Act when consumer data contains information related to accessing, procuring, or searching for services regarding contraception, pregnancy care, and perinatal care, including abortion services. AB 1194 is currently in this Committee.

Prior Legislation:

AB 1242 (Bauer-Kahan, Ch. 627, Stats. 2022) prohibits law enforcement from knowingly arresting a person for performing or aiding in the performance of a lawful abortion or for obtaining an abortion and prohibits specified entities from providing information to

another state or political subdivision thereof regarding an abortion that is lawful under California law, except as provided.

AB 2089 (Bauer-Kahan, Ch. 690, Stats. 2022) *See* Comment 3.

AB 2091 (Mia Bonta, Ch. 628, Stats. 2022), among other things, prohibited compelling a person to identify or provide information that would identify an individual who has sought or obtained an abortion in a state, county, city, or other local criminal, administrative, legislative, or other proceeding if the information is being requested based on another state's laws that interfere with a person's right to choose or obtain an abortion or a foreign penal civil action.

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, 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 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 76, Noes 0)
Assembly Appropriations Committee (Ayes 15, Noes 0)
Assembly Privacy and Consumer Protection Committee (Ayes 10, Noes 0)
Assembly Health Committee (Ayes 13, Noes 0)
**********