Date of Hearing: April 16, 2026
Fiscal: Yes

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Rebecca Bauer-Kahan, Chair
AB 2448 (Berman & Bauer-Kahan) – As Introduced February 20, 2026

**SUBJECT**: Medical information: confidentiality

## SYNOPSIS

*This bill, co-sponsored by Attorney General Rob Bonta and Planned Parenthood Affiliates of California, is intended to clarify existing law. Civil Code Section 56.101 requires electronic health record system providers to "develop capabilities, policies, and procedures" by July 1, 2024, that would protect the sensitive healthcare information of patients by preventing its sharing in a health information exchange. However, there is some ambiguity in the language as to whether providers were required to* enable *the capability by the deadline. This bill clarifies that not only were vendors supposed to develop the capability by July 1, 2024, but they were also supposed to actually enable it.*

*This bill is co-sponsored by Attorney General, Rob Bonta and Planned Parenthood Affiliates of California and enjoys the support of the American College of Obstetricians and Gynecologists, the California Academy of Family Physicians, and the California Women's Law Center, among others. There is no registered opposition.*

*This bill was previously heard by the Health Committee, where it passed on a 12-3 vote.*

**EXISTING LAW**:

1) Establishes the Reproductive Privacy Act, which prohibits the state from denying or interfering with a woman's right to choose or obtain an abortion prior to viability of the fetus, or when the abortion is necessary to protect the life or health of the woman. (Health & Saf. Code § 123460, *et seq*.)

2) Establishes the Confidentiality of Medical Information Act (CMIA) to protect an individual's medical information from unauthorized disclosure by providers of health care. Provides an individual right of action for a patient whose information was disclosed in violation of CMIA's provisions. (Civ. Code § 56 et seq.)

3) Defines "medical information," for the purposes of the CMIA, as any individually identifiable information, in electronic or physical form, that is 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, reproductive or sexual health application information, mental or physical condition, or treatment. Specifies that "individually identifiable" information means medical information that includes any element of personal identifying information sufficient to allow the individual to be identified. (Civ. Code § 56.05(j).)

4) Defines "sensitive services" to mean all health care services related to mental health, behavioral health, sexual and reproductive health, sexually transmitted infections, substance use disorder, gender affirming care, and intimate partner violence. (Civ. Code §56.05(s).)

5) Requires a business that electronically stores or maintains medical information on the provision of sensitive services, including, but not limited to, on an electronic health record system or electronic medical record system, on behalf of a provider of health care, health care service plan, pharmaceutical company, contractor, or employer, to develop capabilities, policies, and procedures, July 1, 2024, to enable all of the following:

   a) Limit user access privileges to information systems that contain medical information related to gender affirming care, abortion and abortion-related services, and contraception only to those persons who are authorized to access specified medical information.

   b) Prevent the disclosure, access, transfer, transmission, or processing of medical information related to gender affirming care, abortion and abortion-related services, and contraception to people and entities outside of this state.

   c) Segregate medical information related to gender affirming care, abortion and abortion-related services, and contraception from the rest of the patient's record.

   d) Provide the ability to automatically disable access to segregated medical information related to gender affirming care, abortion and abortion-related services, and contraception by individuals and entities in another state. (Civ. Code § 56.101 (c)(1).)

6) Prohibits providers of health care, health care service plans, or contractors from disclosing medical information regarding a patient of the provider of health care or an enrollee or subscriber without first obtaining authorization, except as provided. Specifies that a provider of health care, health care service plan, or a contractor must disclose medical information if the disclosure is compelled by:

   a) A court order.

   b) A board, commission, or administrative agency for purposes of adjudication.

   c) A party to a proceeding before a court or administrative agency pursuant to a subpoena, subpoena duces tecum, notice to appear, or any provision authorizing discovery in a proceeding before a court or administrative agency.

   d) A board, commission, or administrative agency pursuant to an investigative subpoena.

   e) An arbitrator or arbitration panel, when arbitration is lawfully requested by either party.

   f) A search warrant lawfully issued to a governmental law enforcement agency.

   g) A patient or patient's representative.

   h) A medical examiner, forensic pathologist, or coroner when requested in the course of an investigation, as specified.

   i) When otherwise specifically required by law. (Civ. Code § 56.10(b).)

7) Requires the California Health and Human Services Agency (CalHHS), on or before July 1, 2022, to establish the California Health and Human Services Data Exchange Framework (DxF) that is to include a single data-sharing agreement and common set of policies and procedures that will leverage and advance national standards for information exchange and data content, and that will govern and require health information exchange (HIE) among health care entities and government agencies in California. (Health & Saf. Code § 130290.)

8) Requires, on or before January 31, 2024, the following health care organizations to execute the data-sharing agreement to participate in data exchange in real time for treatment, payment, or health care operations, as specified:

   a) General acute care hospitals and acute psychiatric hospitals.

   b) Physician organizations and medical groups, as defined.

   c) Skilled nursing facilities that currently maintain electronic records.

   d) Licensed health care service plans and health insurers, as well as Medi-Cal managed care plans, including those that are not state-licensed.

   e) Clinical laboratories. (Health & Saf. Code § 130290.)

9) Requires, by July 1, 2026, the following entities to execute the data-sharing agreement:

   a) A medical foundation exempt from licensure.

   b) Emergency medical services. (Health & Saf. Code § 130290.)

10) Requires, commencing July 1, 2026, compliance with DxF to be required as a condition of continuing, amending, or entering into a new or existing contract for the coverage of or provision of health care services with the Department of Health Care Services, the Public Employees' Retirement System, and the California Health Benefit Exchange. (Health & Saf. Code § 130290.)

11) Exempts the exchange of health information related to abortion, abortion-related services, gender-affirming care, immigration or citizenship status, or place of birth from DxF requirements. (Health & Saf. Code § 130290.)

**THIS BILL**: Clarifies that a business that electronically stores or maintains medical information on the provision of sensitive services, including, but not limited to, on an electronic health record system or electronic medical record system, on behalf of a provider of health care, health care service plan, pharmaceutical company, contractor, or employer was required to enable certain features to protect sensitive services information in an electronic health record by July 1, 2024.

**COMMENTS**:

1) **Author's statement**. According to the author:

   No patient should ever worry that their medical records will be used to criminalize or punish them – or their provider – for health care that is lawful in California. This is why the Legislature passed, and the Governor signed AB 352 requiring businesses that electronically

> store or maintain medical information to enable technological capabilities to protect the privacy and security of medical information related to abortion, contraception, and gender affirming care. In the three years since AB 352's enactment, attacks on reproductive and gender affirming care have only intensified. To date, businesses are at different points in the process of enabling the technology necessary for providers to comply with existing law. AB 2448 reinforces state law to fully protect the privacy and security of their patients' sensitive medical information.

2) **Background**. In 2023, in response to the overturning of *Roe v. Wade* (1973) 410 U.S. 113, 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, AB 352 (Bauer-Kahan; Ch. 255, Stats.2023) was introduced to prevent information on abortion care, gender affirming care, and other sensitive services in health information exchanges from being shared without a patient's permission, especially outside of California. In addition, it required that parties be appropriately authorized to view medical information related to sensitive services, prior to gaining access to the information.

A significant part of the concern was related to providers' use of health information exchanges (HIEs), which are digital services that operate across health organizations to share health care information. HIEs store and exchange information about health conditions, medications, and allergies. It can also include procedures, notes, and lab results. Once an organization is part of an exchange, or a member of a health information network, they have access to the information in the exchange. Because of federal regulations, information that is not exchanged includes substance abuse treatment, which requires written authorization from a patient. In the context of reproductive health care, physicians in abortion ban states could easily see all details of abortion care through HIEs – even if it is unrelated to the patient's care. This created the risk that out-of-state providers will report patients to authorities and endanger patients and providers.

Under the requirements of AB 352, businesses that store and maintain medical information in an electronic health record system were required to "develop capabilities, policies, and procedures" by July 1, 2024, that would allow for the protection of the sensitive healthcare information of patients by preventing its sharing in an HIE. Unfortunately, according to the co-sponsor, Planned Parenthood Affiliates of California:

> California providers have done extensive work with EHR vendors and other entities that exchange health information to work towards businesses meeting their obligations under existing law. To date, these efforts have made progress for California providers and businesses to comply with AB 352 in a way that fulfills the goals of the legislation – to protect patient data. However, the work is ongoing, and providers cannot effectively protect the privacy and security of their patients' records without the technological tools being enabled in EHR and other data sharing systems.

Prior to the Supreme Court's overturning of *Roe v. Wade* in 2022, AB 133 (Committee on Budget; Ch. 143, Stat. of 2021), established the statewide data exchange framework (DxF) and required by July 1, 2022, in consultation with members of a Stakeholder Advisory Group, that the Health and Human Services Agency finalize a data sharing agreement defining parties that will be subject to new data exchange rules and setting forth a common set of terms, conditions, and obligations needed to support secure, real-time access to and exchange of health and social

services information, in compliance with applicable federal, state, and local laws, regulations, and policies.

Subsequently, SB 660 (Menjivar; Ch. 325, Stats. 2025) expanded the universe of entities required to participate in the exchange and comply with the rules of the DxF as a condition for contracting with or providing services through state health care programs commencing July 1, 2026. SB 660 additionally exempted abortion, abortion-related services, gender affirming care, immigration or citizenship status, and place of birth from being exchanged in the framework. However, without the technological capability to segment out sensitive services from their EHRs, providers are faced with an impossible choice, risking the safety of their patients by joining the exchange by July 1 or risk losing their funding.

2) **The need for this bill.** While this bill does not address the core problem of the upcoming July 1, 2026, deadline for signing data sharing agreements, the author and sponsors hope that this clarification to Civil Code Section 56.101 will cause EHR vendors to turn on the capability for providers to protect sensitive medical information by keeping it inaccessible to members of the data exchange. Specifically, this bill clarifies that not only were vendors supposed to develop the capability by July 1, 2024, but they were also supposed to actually enable it.

***ARGUMENTS IN SUPPORT:*** The California Attorney General, co-sponsor of the bill, writes in support:

> Across the country, increasing restrictions on reproductive health care have been accompanied by heightened concerns about the potential misuse of patient data. While existing law requires certain entities to maintain policies and procedures to protect medical information, the next step is to ensure entities are implementing these protections.
>
> AB 2448 ensures these protections are implemented so that providers can segregate and protect reproductive health data when using electronic systems to input patient information. In an era where information sharing through electronic systems keeps expanding, it's imperative to ensure sensitive information isn't unduly exposed. Reproductive data is highly sensitive and personal and should be kept between a patient and provider if the patient so chooses. This fosters trust between the patient and provider which leads to improved communication and patient care. AB 2448 also addresses the threat of hostile anti-abortion actors seeking this type of information with ill intent.
>
> AB 2448 builds on California's ongoing commitment to advance and protect reproductive health care for those who seek and administer it. Reproductive health care is essential to people's autonomy and is foundational to a more equitable society.

Planned Parenthood Affiliates of California further notes:

> This bill clarifies existing law, which says that electronic health record (EHR) vendors must develop the technical capability to protect medical information related to abortion, contraception, and gender affirming care, to make clear that these vendors must enable this capability for their customers so that patient records are protected against unauthorized disclosures. PPAC supports efforts to enable and encourage health information technology to better coordinate patient care, and at the same time protect patient confidentiality – particularly when it comes to sensitive health care services. As health care is becoming increasingly politicized, protecting patient privacy is essential to the care provided by

Planned Parenthood health centers. Patients deserve access to health care without fear of legal or criminal consequences from data sharing.

For Planned Parenthood health centers in California, confidentiality is at the core of being a trusted health care provider, especially given that Planned Parenthood health centers are collectively one of the largest providers of sexual and reproductive health care in the state. PPAC believes that patients

should be able to access reproductive and gender affirming care services safely, comfortably, and without fear of their private information being disclosed and used to harm them. However, without technological capabilities that are responsive to the needs of providers and the patients they serve, providers cannot fully protect the privacy and security of their patients' sensitive medical information. If an individual is uncertain about whether their medical information will be shared, they may feel forced to choose between accessing needed medical care and their privacy and safety.

AB 2448 reinforces existing state law to protect sensitive medical records by clarifying that AB 352 required businesses that electronically store medical information related to sensitive services must both develop and enable the technology needed to protect the privacy and security of sensitive medical records.

**REGISTERED SUPPORT / OPPOSITION**:

**Support**

Attorney General Rob Bonta (Co-Sponsor)
Planned Parenthood Affiliates of California (Co-Sponsor)
Access Reproductive Justice
American College of Obstetricians & Gynecologists - District Ix
California Academy of Family Physicians
California Women's Law Center
Equality California
Reproductive Freedom for All California

**Opposition**

None on file.

**Analysis Prepared by**: Julie Salley / P. & C.P. / (916) 319-2200