Published on *The National Law Review* https://natlawreview.com

California's New Reproductive Privacy Laws AB 352 and AB 254 Create Complexities for Health Information Sharing

Article By:

Daniel F. Gottlieb

Alya Sulaiman

Reuben Bank

In the wake of the Supreme Court of the United States's decision in *Dobbs v. Jackson Women's Health Organization* and the adoption of laws outside California that criminalize most abortions as well as gender affirming care, California Governor Gavin Newsom recently signed Assembly Bill 352 (AB 352) and Assembly Bill 254 (AB 254) into law on September 27, 2023.

Through these new laws, California seeks to mitigate the risk of out-of-state prosecution of individuals seeking abortions or gender affirming care. These bills include significant changes to California privacy and health information interoperability laws that will impact health care providers, health plans, employers, electronic health record (EHR) developers and digital health companies handling medical information related to gender affirming care, abortion, abortion-related services,

sexual health, fertility or contraception.

IN DEPTH

KEY TAKEAWAYS

- EHR developers and digital health companies storing or maintaining medical information for California health care providers, health plans, pharmaceutical companies, employers and certain contractors must develop new privacy, security and data segmentation functionality, policies and procedures by July 1, 2024.
- Health care providers must take steps to limit out-of-state medical information disclosures or cooperation with out-of-state inquiries or investigations consistent with AB 352, with enforcement for noncompliance beginning January 31, 2026.
- Digital health companies, employers and other businesses offering reproductive or sexual health digital services to individuals are subject to certain requirements in the California Confidentiality of Medical Information Act (CMIA) beginning January 1, 2024.
- The California laws are consistent with other states that have adopted special protections for reproductive health information. For example, Maryland enacted a law earlier this year that generally limits health information exchanges and electronic health networks from disclosing information related to abortion care other than for the adjudication of claims or to

a specific treating provider with an appropriate written consent.

AB 352

AB 352 adopts privacy protections for information about gender affirming care, abortion, abortion-related services and contraceptives, and it attempts to prevent out-of-state prosecution against individuals who come to California for abortion or reproductive health-related medical services or gender affirming care.

New Health Information Technology Capabilities, Policies and Procedures

AB 352 amends the CMIA to require EHR developers, digital health companies and other businesses that electronically store or maintain California individuals' medical information on the provision of sensitive services on behalf of health care providers, health plans, pharmaceutical companies, contractors or employers to develop capabilities, policies and procedures by July 1, 2024, to enable the following:

- Limitations on user access privileges to information systems that contain medical information related to gender affirming care, abortion, abortion-related services and contraception only to those persons who are authorized to access the medical information
- Prevention of the disclosure, access, transfer, transmission or processing of such information to any person or entity outside of California
- Segregation of medical information related to gender affirming care, abortion, abortion-related services and contraception

from the rest of a patient’s medical record
- Ability to automatically disable access to segregated medical information related to gender affirming care, abortion, abortion-related services and contraception by individuals and entities in another state

The requirement to segregate a subset of medical information from the rest of a patient’s medical record creates both technical and compliance challenges for health IT developers, digital health companies and other businesses that electronically store medical information. While federal interoperability regulations emphasize the sharing of complete medical records, AB 352 would require the creation of certain data silos that could impact the completeness of an individual’s medical record when viewed by certain users or disclosed to health care providers in other states. AB 352’s data segmentation, access control and disclosure restriction requirements may necessitate complex software development. No algorithm or standardized computational methodology currently exists to automate the reliable classification of medical information related to the provision of sensitive services such as reproductive or gender affirming care. There is a potential for health IT developers to require end-user clinicians and staff to provide context to manually segment and restrict sensitive data elements within a health IT system, which could place a significant burden on these end users.

Notably, AB 352 applies these requirements to businesses that electronically store or maintain medical information on behalf of a wide range of health care industry organizations but not to the health care providers that deploy EHRs and otherwise electronically store or maintain medical information.

In connection with these requirements, California health care organizations should be prepared for potential workflow/functionality changes and fees from health IT developers as they develop new technical capabilities for compliance. AB 352 allows EHR and other health IT developers to charge cost-based fees for the new capabilities consistent with the fees exception to the federal information blocking regulations adopted by the Office of the National Coordinator for Health Information Technology. Interestingly, AB 352 limits the ability of all impacted health IT and digital health companies to charge fees for new capabilities necessitated by AB 352 consistent with federal information blocking regulations, even if a company is not a regulated actor under the information blocking regulations. For more information about the federal information blocking regulations, see our *Special Report*.

Out-of-State Data Disclosures, Inquiries or Investigations

AB 352 further amends the CMIA to prohibit health care providers, health care service plans, contractors and employers (each as defined by CMIA) from cooperating with any inquiry or investigation—or otherwise disclosing medical information—to anyone or any entity from another state that would identify an individual and is related to that individual seeking or obtaining an abortion or abortion-related services that are lawful under California law unless authorized under any of the following conditions:

- In accordance with a written authorization that is valid under CMIA and clearly states that medical information on abortion or abortion-related services may be disclosed, and only to the extent and for the purposes expressly stated in the authorization
- Under the CMIA's preexisting billing and payment-related

confidentiality exceptions to the extent necessary to allow responsibility for payment to be determined and payment to be made or to the extent that it is not further disclosed by the recipient in a way that would violate the CMIA
- Under the CMIA's preexisting confidentiality exceptions for certain quality-related activities for the purpose of accreditation, in reviewing the competence or qualifications of health care professionals, or in reviewing health care services with respect to medical necessity, level of care, quality of care or justification of charges
- Under the CMIA's preexisting confidentiality exception for bona fide research, provided that institutional review boards must consider the potential harm to the patient and the patient's privacy when the research uses data that contains information related to abortion or abortion-related services and is performed out of California

This provision does not prohibit compliance with an investigatory request related to activity that is punishable as a crime in California and took place in California. The provision also does not impact disclosures of medical information to patients or their representatives, even while the requesting individual is out of state. Health care organizations will need to carefully consider how they respond to such patient access requests to ensure that disclosures to third parties, as directed by a patient, comply with AB 352's authorization requirements.

Prior to January 31, 2026, health care providers will not be subject to liability for damages or to civil or enforcement actions for failure to meet the disclosure prohibitions if the provider is working diligently and in good faith to come into compliance. This provision gives providers time to determine the best path to compliance but notably excludes the

other entities subject to the disclosure prohibitions, including health plans, pharmaceutical companies, contractors and employers.

Impact on Health Information Exchange

AB 352 prohibits health care providers, health care service plans, contractors and employers from “knowingly” disclosing or transmitting medical information in an EHR system or through a health information exchange (HIE) that would identify an individual seeking, obtaining, providing, supporting or aiding a lawful abortion to out-of-state individuals, unless authorized. Accordingly, health care providers will need to evaluate the types of medical information transmitted to other EHR systems and HIEs, determine where that information is going and determine how to withhold medical information that cannot be shared by law. This evaluation will be particularly important for health care organizations that participate in national or regional HIEs.

Impact on the California Data Exchange Framework

AB 352 amends the California Health and Safety Code section that authorizes the California Data Exchange Framework (DxF) to provide that its requirement for DxF participants to share health and social services information does not apply to the exchange of health information related to abortion and abortion-related services. Health care organizations and other entities that signed the DxF data sharing agreement are required to exchange data on or before January 31, 2024, so it is unclear how they will operationalize AB 352’s data-sharing restrictions while their health IT developers work to comply with the July 1, 2024, deadline for data segmentation and related privacy functionality. Any fees charged by EHR vendors to enable a regulated entity’s compliance with the DxF are required to be reasonable and

consistent with the federal information blocking regulations.

On a related note, AB 352 directs the DxF stakeholder advisory group to consider whether standards for including EHR vendors in the DxF would be appropriate and, if determined to be appropriate, develop those standards. If the stakeholder advisory group develops standards for including EHR vendors in the DxF, AB 352 would require EHR vendors to sign the DxF data sharing agreement within 12 months of the completion of those standards.

For more information about the California DxF, see our *On the Subject*, "10 Things Providers Should Know About California's Data Exchange Framework."

AB 254

The CMIA imposes privacy requirements on certain health care providers, pharmaceutical companies, California health care service plans and other entities. It does not regulate all California businesses.

The CMIA prohibits regulated entities from disclosing "medical information" in their possession regarding a patient, enrollee or subscriber without the individual's prior authorization unless an exception applies. The CMIA further requires those entities to create, maintain, store or destroy medical information in a manner that preserves its confidentiality. As discussed below, effective January 1, 2024, AB 254 revises the CMIA to regulate companies providing reproductive or sexual health digital services and data considered to be reproductive or sexual health application information.

Expansion of CMIA-Regulated Entities

AB 254 amends the CMIA to add a new class of regulated entities. Specifically, AB 254 requires “any business that offers a reproductive or sexual health digital service to a consumer” to comply with the CMIA requirements applicable to health care providers. A reproductive or sexual health digital service is 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. This could include services individuals use to manage or track their menstrual, fertility, or pregnancy information, or other sexual health data. These services include mobile applications or websites that collect reproductive or sexual health application information from consumers. This expansion is significant for digital health companies and employers offering reproductive or sexual health digital services in California that might not have previously addressed the CMIA’s requirements in their privacy compliance programs.

As a result of this expanded scope, entities offering reproductive or sexual health digital services must comply with the CMIA’s:

- Prohibition on the disclosure of medical information, except as permitted by one of the CMIA’s disclosure exceptions or an individual’s authorization
- Requirement to not “intentionally share, sell, use for marketing, or otherwise use medical information for a purpose not necessary to provide health care services to the patient,” except to the extent expressly authorized by the individual

Consequently, AB 254 limits the ability of a reproductive or sexual health digital service to collect and sell the data collected from

individuals. To the extent that a mobile application or website also collects other types of medical information, AB 254 will impose a burden upon them to bifurcate data (especially reproductive or sexual health information) from California individuals to comply with the CMIA.

Expansion of the Definition of Medical Information

The CMIA currently defines "medical information" to include individually identifiable information about an individual's medical history, mental health application information, mental or physical condition or treatment. Effective January 1, 2024, AB 254 adds "reproductive or sexual health application information" to that definition. Reproductive or sexual health application information is information about a consumer's reproductive health, menstrual cycle, fertility, pregnancy, pregnancy outcome, plans to conceive or type of sexual activity collected by a reproductive or sexual health digital service, including information from which one can infer someone's pregnancy status, menstrual cycle, fertility, hormone levels, birth control use, sexual activity or gender identity. Consequently, health care providers and other CMIA-regulated entities must begin protecting reproductive and sexual health application information as they would other types of medical information protected by CMIA.

NEXT STEPS

- Health IT developers and digital health companies that serve organizations in California will need to begin evaluating their technical capabilities, policies and procedures to determine how they will comply with the data segmentation and other privacy requirements of AB 352. These entities should also carefully calculate any fees for new functionality or technical

capabilities required under AB 352 for compliance with limitations in the federal information blocking regulations.

- Health care providers and health plans in California will need to map their data flows, especially those that result in out-of-state disclosures of medical information, and to take steps to "diligently and in good faith" comply with the disclosure prohibitions in AB 352.
- Health care providers, health plans, pharmaceutical companies, contractors and employers should reach out to their IT vendors to inquire about the vendors' plans to comply with the requirements in AB 352 before the July 1, 2024, compliance deadline. Entities participating in the California DxF will need to evaluate how to meet their information-sharing commitments beginning on January 31, 2024, given the potential functionality gap to support the special handling of data related to reproductive health and gender affirming care.
- Digital health companies and employers that offer reproductive or sexual health digital services to individuals in California should evaluate their compliance with the CMIA's requirements for health care providers, including certain limitations on the use and disclosure of medical information.

National Law Review, Volumess XIII, Number 334