Articles + Publications | January 23, 2024

New California Law Imposes Significant Data Management Requirements for Sensitive Health Data

WRITTEN BY

Erin S. Whaley | Brent T. Hoard | Emma E. Trivax

On January 1, California's Assembly Bill No. 352 (AB 352) went into effect, introducing significant changes to the handling and sharing of sensitive health information — particularly information related to reproductive health services. Under California's existing Reproductive Privacy Act and the Confidentiality of Medical Information Act (CMIA), individuals have a fundamental right to privacy in their reproductive decisions, and unauthorized disclosure of medical information is generally prohibited.

AB 352 will impact both traditional and nontraditional health care entities. However, because AB 352 amends several existing California statutes and creates a new one, the scope of the various changes is different depending on the applicable statute. Thus, it is important to determine whether your business would fall under all, some, or none of the new/amended California laws.

4 Key Requirements for Health Care Entities

1. Enhanced Security Measures for Certain Businesses

By July 1, certain businesses that electronically store or maintain medical information related to gender-affirming services, abortion and abortion-related services, and contraception, must (1) limit user access privileges, (2) prevent the sharing of medical information to persons and entities outside of California; (3) segregate medical information from the rest of the patient's record, if the remaining record must be disclosed pursuant to a valid request; and (4) provide the ability to automatically disable access to segregated medical information from individuals and entities outside of California.[1] Whether this law applies to businesses located outside of California that serve California residents is unclear.

These requirements apply to a business that electronically stores or maintains medical information on the provision of sensitive services. A business, as defined in Cal. Civil Code § 56.06, includes, but is not limited to: businesses that maintain medical information for individuals or providers, offer software or hardware to manage medical information, or provide a digital service related to reproductive or sexual health. Despite ambiguities in the definition of business, those likely to be required to comply with these enhanced security measures include health care providers, pharmacies, and companies that provide electronic medical records, e-prescribing systems, patient-facing applications, and more.

2. Prohibition on Cooperation With Out-of-State Inquiries

Health care providers, service plans, contractors, and employers are prohibited from cooperating with any inquiry or investigation by, or providing medical information to, an individual, agency, or department from another state or a federal law enforcement agency that would identify an individual seeking or obtaining an abortion or abortion-related services that are lawful under California law, unless the request for medical information is authorized under existing law provisions.[2]

3. Prohibition on Disclosure of Medical Information

Health care providers, service plans, pharmaceutical companies, contractors, and employers are prohibited from knowingly disclosing, transmitting, transferring, sharing, or granting access to medical information in an electronic health records system, or through a health information exchange, that would identify an individual, and that is related to an individual seeking, obtaining, providing, supporting, or aiding in the performance of an abortion that is lawful under California law to any individual or entity from another state, unless authorized under specific conditions.[3]

Health care providers[4] are exempt from liability for damages or from civil or enforcement actions relating to cooperating with, or providing medical information to, another state or a federal law enforcement agency before January 31, 2026, if they are working diligently and in good faith to comply with the prohibition.[5] This grace period allows time for health care providers to create the appropriate systems and policies to comply with the new requirement.

4. Exclusion From Automatic Data Sharing.

The bill excludes the exchange of health information related to abortion and abortion-related services from being automatically shared on the California Health and Human Services Data Exchange Framework as required under applicable law.[6]

5 Action Items to Prepare

Entities that may be impacted by AB 352 can consider the following action items to prepare:

1. Determine whether you or your organization fall under the scope for any of the four new requirements. This is crucial, especially for nontraditional health care entities that might not typically consider compliance with various health care laws and regulations.

2. Undertake a detailed data element inventory to understand the types and locations of in-scope data within your record-keeping environment.

3. Develop and implement appropriate technical controls to identify, manage, and segregate relevant data, ensuring proper access controls and provisioning processes are in place.

4. Review and revise existing procedures for individual rights requests (or develop a separate process) to identify and address requests that may be in scope of the new law.

5. Incorporate reminders about these restrictions in training sessions (*e.g.*, annual privacy and security training) for relevant members of the workforce to ensure continued awareness.

Conclusion

The changes introduced by AB 352 are substantial. Entities should quickly determine whether the new law will apply to their businesses in order to timely address the potentially significant modifications to their systems and policies. Notably, entities subject to the enhanced security feature requirement will have only six months to develop and implement these security features.

For more information about AB 352 and other questions related to health care data privacy and security, please contact erin.whaley@troutman.com, brent.hoard@troutman.com, and emma.trivax@troutman.com.

---

[1] Cal. Civil Code § 56.101(c).

[2] Cal. Civil Code § 56.108(c); see also Cal. Civil Code § 56.110.

[3] Cal. Civil Code § 56.110.

[4] Cal. Civil Code § 56.05.

[5] Cal. Civil Code § 56.110(d).

[6] Cal. Health & Safety Code § 130290. Required to participate in the exchange are: general acute care hospitals, physician organizations and medical groups, skilled nursing facilities, health care services plans and disability insurers that provide hospital, medical, or surgical coverage and are regulated by the Department of Managed Health Care or the Department of Insurance, clinical laboratories, and acute psychiatric hospitals.

RELATED INDUSTRIES + PRACTICES

- Data + Privacy
- Health Care + Life Sciences
- Health Care Regulatory