Now & Next
Health Information & Data Privacy Alert

May 15, 2026

CMIA data breach standard clarified by California Supreme Court

By Harsh Parikh, Andrew Winetroub, Taylor Hooks, and April Yang

The California Supreme Court recently redefined the CMIA pleading standard and scope of covered entities in data breach litigation.

What's the impact?

- The court lowered the bar for asserting CMIA claims; plaintiffs no longer need to show data was actually viewed, just that it faced a "significant risk" of unauthorized access.
- Not every company handling health data is covered—some platforms may fall outside the CMIA if their main purpose isn't medical care or record management.
- The decision previews future CMIA class action litigation involving "emerging technologies."

On May 14, 2026, the California Supreme Court issued a significant opinion interpreting the Confidentiality of Medical Information Act (CMIA; Cal. Civ. Code §§ 56 *et seq.*) in the context of a data breach involving an educational technology company. The decision in *J.M. v. Illuminate Education, Inc.* (California Supreme Court, Case No. S286699) adopts a plaintiff-friendly standard

for pleading and establishing a breach of confidentiality under CMIA § 56.101, narrows the definition of covered "providers of healthcare," and limits private rights of action under the Customer Records Act (CRA). The state Supreme Court's decision is expected to have immediate implications for class action litigation in data breaches involving medical information, including for healthcare providers and in the ed-tech, health-tech, and consumer-facing digital health sectors.

Background on California's Confidentiality of Medical Information Act (CMIA)

Enacted in 1979 (and significantly amended in 1993, 1999, 2007, and 2013), the CMIA is one of the nation's strongest state-level medical privacy statutes. It supplements (and in some respects exceeds) federal HIPAA protections by imposing strict confidentiality obligations on "providers of healthcare," healthcare service plans, contractors, pharmaceutical companies, and certain other entities that handle individually identifiable medical information (defined broadly to include any information regarding a patient's medical history, mental or physical condition, or treatment).

KEY PROVISIONS OF THE CMIA

- Prohibition on unauthorized disclosure (§ 56.10): Covered entities generally may not disclose medical information without the patient's written authorization (subject to limited exceptions).
- Duty to preserve confidentiality (§ 56.101): Entities must create, maintain, store, etc., medical information "in a manner that preserves the confidentiality of the information." Negligent handling triggers liability.
- Private right of action (§ 56.36(b)): Individuals whose information is "negligently released" may recover nominal damages of $1,000 per violation (without any need to show actual or threatened harm), plus actual damages, attorneys' fees, and other relief in appropriate cases.
- Expanded coverage (§ 56.06): Amendments extended the statute beyond traditional medical providers to businesses organized to maintain medical information for patient management or diagnosis/treatment purposes, and to vendors of personal health record software/hardware (including mobile apps).
- The CMIA is frequently invoked in data breach class actions because it provides a private right of action with relatively low barriers to substantial nominal damages and, now under *Illuminate*, does not require pleading or proof of actual viewing or misuse in every instance.

Summary of the California Supreme Court's Decision in *J.M. v. Illuminate Education, Inc.*

Plaintiff J.M. (a minor and student) alleged that Illuminate Education, Inc.—an ed-tech company providing student data platforms to school districts—suffered a data breach exposing students' medical information (including certain diagnoses and treatment plans). J.M. brought class claims under the CMIA (§§ 56.10 and 56.101) and the CRA for negligent data handling and delayed breach notification.

The trial court sustained Illuminate's demurrer without leave to amend. The Court of Appeal reversed. The California Supreme Court reversed the Court of Appeal and held that J.M. failed to state viable claims under either statute (while remanding for consideration of potential amendment).

KEY HOLDINGS

No "Actually Viewed" Requirement for § 56.101 Claims; New "Significant Risk" Standard

The Court rejected a widely-cited and frequently relied-upon line of Court of Appeal decisions that had required plaintiffs to allege that unauthorized third parties "actually viewed" their information.

- A breach of confidentiality under § 56.101 occurs when medical information is "exposed to a significant risk of unauthorized access or use."
- Factors include the nature, duration, and extent of the breach, mitigation efforts, and whether the data was targeted (vs. incidental to hardware theft).
- Mere negligent loss of possession is neither automatically sufficient nor irrelevant; all circumstances are considered.
- The Court determined this standard aligns with the statute's remedial purpose and nominal-damages provision, which does not require actual harm.

Illuminate Is Not a "Provider of Health Care" Under § 56.06(a) or (b)

The Court held that J.M. failed to allege facts showing Illuminate is a business "organized for the purpose of maintaining medical information" in order to make it available (at the individual's or provider's request) for (i) the individual to manage their own information or (ii) diagnosis/treatment of a medical condition of the individual.

- Illuminate's platform primarily served educational purposes (such as dyslexia screening, progress monitoring, and educational planning for school districts and educators).
- Access by students/parents was incidental and tied to educational goals, not individual

health record management or medical diagnosis/treatment.

- Legislative history (e.g., MedicAlert services, personal health records, mobile health apps) confirms the statute targets entities enabling patient-controlled or medically focused use of records—not ed-tech vendors.

The Court also rejected that Illuminate was covered by the CMIA under § 56.13 (J.M. failed to allege any authorization by which Illuminate received his medical information) or § 56.11(c) (J.M. failed to allege that Illuminate is a healthcare provider, healthcare service plan, pharmaceutical company, contractor, or other entity that seeks authorization to disclose protected health information).

No CRA Claim

J.M. was not Illuminate's "customer" (§ 1798.80(c)) because he did not provide personal information to Illuminate to purchase or obtain services from it; rather, the school district was the customer.

CONCURRING OPINION (GROBAN, J.)

Justice Groban agreed with the majority in the decision but, on the issue of the new standard for § 56.101 created by the Supreme Court, he stated that the "significant risk of unauthorized access or use . . . must be grounded in facts showing that unauthorized access to or use of the data is reasonably likely under the circumstances." Justice Groban's concurring opinion is also notable for emphasizing that a "disclos[ure]" under § 56.10(a) cannot be shown when medical information is obtained through an unauthorized cyberattack.

Potential Implications for CMIA Class Action Litigation

EASIER PLEADING AND SURVIVAL OF DEMURRERS IN DATA BREACH CASES

The "significant risk" standard lowers the bar for plaintiffs to allege a § 56.101 violation. Class counsel will likely argue that most sophisticated cyber breaches (especially those involving targeted access to medical data) inherently create such a risk. Expect more CMIA class actions to survive pleading challenges, increasing pressure for early resolution.

NARROWER CMIA APPLICABILITY TO NON-HEALTHCARE ENTITIES

Businesses that handle medical information incidentally (e.g., ed-tech, fitness apps, wellness platforms, or SaaS providers to schools/employers) may now have stronger arguments to defeat CMIA claims by showing they fall outside § 56.06's purpose requirements. Companies should carefully review their business models, data flows, and contracts with schools or other entities.

CONTINUED IMPORTANCE OF AUTHORIZATION AND "DISCLOSURE" CLAIMS

The concurrence reinforces that pure data breaches may not trigger § 56.10 liability (absent affirmative disclosure). Plaintiffs may shift their focus to negligent preservation claims under § 56.101.

Strategic considerations for defendants

- Scrutinize whether the entity qualifies as a § 56.06 "provider of healthcare."
- Document robust data security and breach-response measures to argue lack of "significant risk."
- Consider CRA applicability carefully—only true "customers" have a private right of action.

BROADER IMPACT

The ruling may influence how courts interpret similar statutes elsewhere and could prompt legislative clarification or further amendments to § 56.06. The California Attorney General's office (which filed an amicus brief supporting the "significant risk" approach) may also increase enforcement activity.

The California Supreme Court previewed what is likely to be an emerging issue in CMIA class action litigation, specifically pointing to "evolving technologies" such as "artificial intelligence or automated cybercrime" as facilitating unauthorized use of medical information "without anyone actually viewing the information."

Recommended actions

- Health-tech, ed-tech, and other vendors handling California medical information should review CMIA compliance programs, vendor agreements, and breach-notification protocols.
- Companies involved in pending or anticipated CMIA class actions should promptly assess the impact of this decision on pending motions and settlement strategy.
- Counsel should monitor lower-court applications of the "significant risk" standard and any legislative response.

Nixon Peabody's healthcare and data privacy lawyers can help healthcare providers and other organizations that maintain sensitive data assess how this decision might affect your organization's operations or litigation exposure, strengthen privacy and security programs to reduce breach risk, and prepare incident-response and notification plans.

For more information on the content of this alert, please contact your Nixon Peabody attorney or:

Harsh Parikh
213.629.6108
hparikh@nixonpeabody.com

Taylor Hooks
213.629.6079
thooks@nixonpeabody.com

Andrew Winetroub
415.984.8271
awinetroub@nixonpeabody.com

April Yang
213.629.6003
ayang@nixonpeabody.com