Calif. Ruling Lowers Bar For Health Data Breach Claims

By **Naomi May, Matt Nguyen and Vanessa Agudelo** (June 1, 2026)

Naomi May

Matt Nguyen

Vanessa Agudelo

On May 14, the California Supreme Court **issued its opinion** in J.M. v. Illuminate Education Inc., delivering an important and nuanced ruling for companies that maintain health-related data but do not consider themselves healthcare businesses.

At stake was whether all types of companies — including education technology providers, data analytics providers, cloud-based platform vendors and other non-healthcare businesses that happen to maintain health-related data of Californians — can be sued as "providers of healthcare" under Section 56 of California's Confidentiality of Medical Information Act, and, as a result, be subject to its data protection obligations and significant civil exposure.

The court also weighed in on these companies' obligations to safeguard health-related data and promptly disclose breaches under both the CMIA and the California Customer Records Act.

While the court rejected the plaintiff's argument and the lower court's finding that companies that maintain health data can be held liable as providers of healthcare under the CMIA and CRA, the court also adopted a new and more plaintiff-favorable standard for breach of confidentiality that companies maintaining any health-related data should take steps to address.

Background

The central question in the case was whether a software company that maintains personal and medical information to support students' educational needs is subject to liability under the CMIA and CRA when that information is exposed through a data breach.

Illuminate is a California-based K-12 education technology company that offers software programs, applications and technology support to school districts to facilitate student learning and academic assessment. Notably, Illuminate does not employ, contract or work with any medical providers. Nor does Illuminate offer or provide any medical services.

In January 2022, Illuminate experienced a cyberattack that compromised educational and personal information belonging to students across several school districts.

Following the data breach, a student plaintiff — J.M. — filed a class action, alleging that Illuminate had maintained students' medical information, and had failed to secure that data against unauthorized access. J.M. further alleged that Illuminate waited approximately five months before notifying affected students of the breach. Based on these allegations, J.M. alleged that Illuminate violated both the CMIA and the CRA.

The CMIA prohibits healthcare providers from disclosing a patient's medical information without authorization, except under certain enumerated circumstances.

Under the CMIA, a company is subject to $1,000 in nominal damages for each and every unauthorized disclosure, such that a data breach in a class action context could generate massive liability for companies that maintain even incidental health-related data.

The CRA provides additional data protection for customers whose personal information is maintained by businesses they transact with.

Illuminate moved to dismiss, arguing that it was not a provider of healthcare subject to the CMIA because it had no involvement in the delivery of healthcare services. In addition, Illuminate also argued that J.M. failed to show that an actual disclosure had occurred or that an unauthorized party had actually viewed any data. Illuminate further contended that the student plaintiff was not its customer for purposes of the CRA, as its contractual relationships were with the school districts, rather than individual students.

The trial court dismissed the case, finding that Illuminate was not a provider of healthcare under the CMIA, and that the plaintiff had failed to state a claim under either the CMIA or CRA.

The California Court of Appeal's Broad Ruling

In 2024, the Court of Appeal of the State of California, Fourth Appellate District, reversed the trial court's decision and revived J.M.'s class action.[1] In doing so, it adopted an expansive interpretation of entities subject to liability under the CMIA.

According to the Fourth Appellate District, the CMIA extends beyond medical providers, and any business qualifies as a provider of healthcare under the CMIA if it either maintains medical information used "for the diagnosis" of any person, or provides "software or hardware" for that purpose.

Based on the Fourth Appellate District's ruling, even if a company does not employ or contract with medical professionals, diagnose patients, or otherwise act as a medical provider, the company is nevertheless subject to civil exposure under the CMIA as a provider of healthcare if it maintains health-related data for the diagnosis of an individual, or that provides software or hardware for that purpose.

Additionally, even if a business does not meet the definition of a healthcare provider or maintain medical data for the covered purposes, the Fourth Appellate District held that the CMIA broadly applies to businesses that receive medical information or seek authorization for the "disclosure of protected health information."

Applying both of these lines of reasoning, the court held that Illuminate is subject to liability as a provider of healthcare because it used students' mental health records to diagnose their educational needs and progress. It further held that the CMIA also applies to Illuminate as a recipient of medical information.

Furthermore, in assessing whether J.M. had showed a sufficient violation of the CMIA and a related injury to state a claim, the Fourth Appellate District held that a violation of the CMIA does not require proof of an affirmative communicative act by the entity that has maintained the medical information, and that negligent release is sufficient.

In addition, the Fourth Appellate District also held that J.M. was an intended beneficiary under the CRA and thus, CRA obligations also applied. Although Illuminate's contractual

relationship was with the school districts, the court reasoned that the ultimate customers were the "consumers, and beneficiaries of its educational services … the students who trusted Illuminate to protect their information."

The court further found that Illuminate fell within the scope of the then-operative CRA timing standard requiring businesses to disclose security breaches "in the most expedient time possible and without unreasonable delay."[2] According to the court, Illuminate's alleged five-month delay in disclosing the breach to the students violated the CRA.

The California Supreme Court's New Standard To Analyze CMIA Violations

The California Supreme Court granted Illuminate's petition for review to decide whether companies like Illuminate qualify as providers of healthcare under the CMIA.

On May 14, the court held that the CMIA does not apply to Illuminate. Illuminate is not a provider of healthcare under the CMIA because its services were provided to and used by educators for educational planning but not for provision of healthcare services. The court declined to address whether Illuminate qualified as a recipient of medical information or a contractor, as those claims were not raised.

The court also held that a CMIA violation does not require proof of an affirmative act of disclosure or actual unauthorized viewing, but mere loss of possession is not always sufficient either. Despite rejecting the CMIA claim, the court clarified the standard under Section 56.101 of the CMIA: a violation requires showing a significant risk of unauthorized access or use. Actual unauthorized access is not required, but mere loss of possession is not always sufficient. Relevant factors include the form, duration and extent of the breach, and any mitigation efforts.

And finally, it held that the CRA's breach notification requirements do not extend to individuals who are not actual customers of the breached business. J.M. lacked standing under the CRA because he was not Illuminate's customer. It was the Ventura County Office of Education that contracted with Illuminate. The court rejected J.M.'s "intended beneficiary" argument, noting the Legislature deliberately chose "customer" over the broader term "consumer."

The Supreme Court reversed the judgment of the Fourth Appellate District and remanded the matter for further proceedings consistent with its opinion, leaving to the lower courts the question of whether J.M. may amend his CMIA and CRA allegations.

What This Ruling Means for Companies

Although this ruling offers protection for companies that maintain health-related data but do not provide healthcare services, it also introduces a more plaintiff-friendly standard for future data breach litigation, and one that companies maintaining health-related data of Californians should be aware of. The following are a few steps to understand the newly heightened exposure under the CMIA and CRA.

Review descriptions of services.

A company might not be a healthcare provider under the CMIA even if it maintains health-related data, but the analysis is fact-specific and depends heavily on how the services are used and by whom. The court focused heavily on the function and intended end user of Illuminate's product. If a company's marketing materials, product documentation and

contracts describe its services in ways that could suggest a medical or diagnostic purpose — even loosely — that language could expose the company to CMIA liability.

In addition, even if a company does not consider itself a healthcare provider, if customers use its services to provide healthcare services, the company could still face risk under the CMIA. Companies should also be aware that other CMIA provisions under Section 56.13, which were not addressed by the California Supreme Court, may further broaden the CMIA's applicability in the future.

Review breach prevention and response practices.

The new "significant risk" standard means a company can face CMIA liability even if no one actually viewed the exposed data, so breach prevention and rapid response are more important than ever.

Because the court recognized affirmative mitigation efforts as an explicit factor in whether a violation has occurred, a prompt and thorough response focused on containment, notification and remediation can meaningfully reduce legal exposure. Importantly, the concurring opinion signals that robust encryption of sensitive data may be a meaningful shield against liability.

Prepare for AI-facilitated data breach claims.

The court flagged an emerging and important risk: Data breaches resulting in unauthorized use of medical information may be facilitated by artificial intelligence or automated cybercrime, without anyone actually viewing the information.

This observation directly informed the court's rejection of the "actually viewed" standard because AI-driven attacks can exploit stolen data without any human ever accessing it, so requiring proof of actual viewing would effectively immunize bad actors using automated tools.

Companies should assess whether their current security posture and incident response plans account for AI-enabled threats, including automated exfiltration and large-scale pattern recognition attacks on health-related datasets.

Review vendor contracts.

In business-to-business relationships, end users whose data is being processed might not have standing to sue a company directly under the CRA, but this does not eliminate risk. Institutional clients can still sue if the breach originates from a company's system. Companies should make sure vendor agreements and data processing agreements clearly allocate responsibility for breach response costs, notification obligations and litigation exposure.

Ultimately, proactive steps matter. In light of the legal standard newly articulated by the California Supreme Court, it is an ideal time for companies to review their data security practices, incident response protocols, data classification policies and vendor agreements.

If there is a chance a company's data-handling activities could bring it within the CMIA or CRA's scope — even as an education technology service provider — now is the time for it to assess and address that risk.

Naomi May is a partner, and Matt Nguyen and Vanessa Agudelo are associates, at Cooley LLP.

Cooley associate Rebecca Khan contributed to this article.

[1] J.M. v. Illuminate Education Inc.,103 Cal.App.5th 1125, 1129 (2024).

[2] Effective January 1, 2026, the California Legislature amended the CRA's disclosure period to 30 days.