IN THE SUPREME COURT OF CALIFORNIA

J.M., a Minor, etc.,
Plaintiff and Appellant,
v.
ILLUMINATE EDUCATION, INC.,
Defendant and Respondent.

S286699

Second Appellate District, Division Six
B327683

Ventura County Superior Court
56-2022-00567324-CU-MC-VTA

May 14, 2026

Justice Liu authored the opinion of the Court, in which Chief Justice Guerrero and Justices Corrigan, Kruger, Groban, Evans, and Buchanan* concurred.

Justice Groban filed a concurring opinion.

---

* Associate Justice of the Court of Appeal, Fourth Appellate District, Division One, assigned by the Chief Justice pursuant to article VI, section 6 of the California Constitution.

J.M. v. ILLUMINATE EDUCATION, INC.

S286699

Opinion of the Court by Liu, J.

Defendant Illuminate Education, Inc. (Illuminate) is an educational technology company that collects data on individual students, including medical information, in the course of providing support and services to help school districts meet students' educational needs. Illuminate provides such services to the Ventura County Office of Education, which serves the school district where plaintiff J.M. was a student. In 2022, Illuminate became aware of a data breach that resulted in unauthorized access to students' medical information, including J.M.'s. J.M., through his guardian ad litem, brought a class action suit against Illuminate for violations of the Confidentiality of Medical Information Act (CMIA; Civ. Code, § 56 et seq.) and the Customer Records Act (CRA; Civ. Code, § 1798.80 et seq.). The trial court dismissed the suit for failure to state a claim; the Court of Appeal reversed. We granted review to decide whether J.M. has stated a cognizable claim under the CMIA or the CRA.

We hold as follows: First, J.M. has not stated a valid claim under the CMIA because he has not sufficiently alleged that Illuminate is a "provider of health care" within the meaning of Civil Code section 56.06. (All undesignated statutory references are to the Civil Code.) Second, in order to establish a failure to preserve the confidentiality of medical information under the CMIA (§ 56.101), a plaintiff does not need to allege that the information was actually viewed by an unauthorized third

party; confidentiality is breached when the information is exposed to a significant risk of unauthorized access or use. Third, because J.M. has not sufficiently alleged that he is Illuminate's "customer" within the meaning of the CRA (see §§ 1798.80, subd. (c) [defining the term], 1798.84, subd. (b) [authorizing civil suits by injured "customer[s]"]), he has not stated a cause of action against Illuminate under the CRA arising from the data breach.

I.

"In considering whether a demurrer should have been sustained, 'we accept as true the well-pleaded facts in the operative complaint.' " (*Beacon Residential Community Assn. v. Skidmore, Owings & Merrill LLP* (2014) 59 Cal.4th 568, 571.) The trial court granted Illuminate's demurrer without leave to amend on the ground that J.M.'s first amended complaint was insufficient to state a claim for relief and the proposed second amended complaint would not cure the defects. The Court of Appeal held that the trial court abused its discretion by sustaining the demurrer without leave to amend because J.M. could cure the defects in the first amended complaint. (*J.M. v. Illuminate Education, Inc.* (2024) 103 Cal.App.5th 1125, 1129 (*Illuminate*).) Accordingly, we assume as true the properly pleaded facts in the second amended complaint, as described below. (See *Goonewardene v. ADP, LLC* (2019) 6 Cal.5th 817, 832–833.)

Illuminate "is an education company that provides applications and technology support to schools and school districts," including J.M.'s school district. To do so, "Illuminate maintains a nationwide internet platform that stores and assesses data concerning students in grades K-12 . . . , with

access provided to educators, students and parents as an aid to educational evaluation, monitoring of progress, and determining an educational plan." The programs help educators identify student needs and deficits, monitor academic and social-emotional progress, facilitate student evaluations, and develop educational and behavior-management plans. For example, "Illuminate provides 'educators with the right dyslexia screening data' because 'educators need the right data about students' early reading skills to identify if they are exhibiting deficits associated with dyslexia.' With its 'dyslexia screening, progress monitoring, and aligned interventions, students can make significant reading improvements.' " Illuminate collects personal data about individual students, including medical information, to provide these services.

J.M. attended a school in a district governed by the Ventura County Office of Education, which contracts with Illuminate for its services. He provided his "medical information," including his "medical history, mental or physical condition, or treatment," to the district, which in turn provided that information to Illuminate.

On January 8, 2022, Illuminate became aware of "suspicious activity" in a set of applications it maintained. Illuminate "immediately took steps to secure the affected applications and launched an investigation." On March 24, 2022, the investigation "confirmed that certain databases containing potentially protected student information were subject to unauthorized access between December 28, 2021, and January 8, 2022." About 12 days later, Illuminate "began the process of notifying [the] Ventura County Office of Education" of the breach.

On June 10, 2022, Illuminate sent a written notice informing J.M.'s guardians, among others, about the data breach. The notice explained that Illuminate was "now notifying you of this incident because our investigation has determined that your minor's information was contained in the affected databases." Those databases "may have contained the following: your minor's name, academic and behavior information, enrollment information, accommodation information, special education information, medical information, and/or student demographic information." The notice further said there was "no evidence that any information was subject to actual or attempted misuse."

Following the breach, J.M. alleges he "has received numerous solicitations by mail from third parties at an address he only provided to [Illuminate] through the Office of Education."

J.M. sued Illuminate, alleging that he and a putative class of all California citizens who were "registered with their school districts on or before December 28, 2021, and who received notices" of the data breach were "placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft" by Illuminate's negligent data handling. The complaint claimed that Illuminate is a provider of health care that disclosed medical information and negligently handled medical information in violation of sections 56.10 and 56.101 of the CMIA. It also claimed that Illuminate failed to disclose the data breach expediently, as required by the CRA.

Illuminate demurred, arguing that it was not covered by the CMIA, that J.M. could not sue under the CRA, and that J.M. did not allege sufficient injuries under either statute. In

response, J.M. lodged a second amended complaint alleging that Illuminate was a "provider of health care" under section 56.06, subdivision (a) or (b). It also included additional facts regarding the data breach — specifically, that J.M. is "informed and believes that not only was his confidential medical information stolen, but it was actually viewed," because he had "received numerous phone calls from solicitors regarding phantom Amazon accounts and other odd phone calls."

The trial court sustained the demurrer without leave to amend after determining that the first amended complaint was insufficient and that the second amended complaint would not cure the defects. It agreed with Illuminate that J.M. did not adequately allege Illuminate was a "provider of health care," "contractor," or "administrator" within the meaning of the CMIA. (See §§ 56.05, subds. (m), (d), 56.06, 56.26.) Additionally, the court concluded J.M. did not allege the sort of "disclosure" or "release" of information that would violate the CMIA. (See §§ 56.10, 56.36, subd. (b).) As to the CRA claim, the court concluded that Illuminate did not "own[] or license[]" the breached data (§ 1798.82, subd. (a)(1)) and that Illuminate did not owe a duty to J.M. under the CRA because its customer was the Ventura County Office of Education, not J.M. It also concluded J.M. had not sufficiently alleged injury under this statute.

The Court of Appeal reversed, concluding "(1) Illuminate falls within the scope of the CMIA and CRA; (2) J.M. stated sufficient facts to state causes of action under the CMIA and CRA; and (3) the trial court abused its discretion by sustaining the demurrer without leave to amend." (*Illuminate*, *supra*, 103 Cal.App.5th at p. 1129.) The court held that Illuminate falls within section 56.06's coverage of " 'any business' that

maintains medical information used 'for the diagnosis' of an individual [citation], or that provides 'software or hardware' for that purpose [citation]." (*Illuminate*, at p. 1132, quoting § 56.06, subds. (a), (b).) The court also held that Illuminate is "a 'recipient of medical information' under section 56.13" and " 'any other entity' that [had sought] an authorization for 'disclosure of protected health information' " under section 56.11, subdivision (c). (*Illuminate*, at p. 1132, italics omitted.) Further, the court held that J.M.'s allegations of Illuminate's negligent storage of medical information leading to unauthorized access were sufficient to state a violation of the CMIA and that he had alleged the requisite harm under sections 56.10 and 56.101. (*Illuminate*, at pp. 1133–1134.)

With respect to the CRA, the court found that J.M. "was an intended beneficiary" of the CRA, which requires prompt disclosures of certain breaches by businesses owning or licensing data. (*Illuminate*, *supra*, 103 Cal.App.5th at p. 1135.) The court described J.M. and the students who gave Illuminate their information as the "ultimate 'customers,' consumers, and beneficiaries" of Illuminate's services. (*Ibid.*) The court further held that "[a] five-month disclosure delay supports a cause of action under the CRA because such a delay prevents victims from taking prompt steps to protect their personal information. . . . This resulted in a 'credible threat' of 'immediate harm' to the plaintiff." (*Ibid.*, citation omitted.)

We granted review.

II.

The Legislature enacted the CMIA to "protect the confidentiality of individually identifiable medical information obtained from a patient by a health care provider, while at the

same time setting forth limited circumstances in which the release of such information to specified entities or individuals is permissible." (*Loder v. City of Glendale* (1997) 14 Cal.4th 846, 859.) Originally enacted in 1979, the statute has been amended several times to expand its scope. As relevant here, the Legislature added section 56.06 in 1993, extending the statute's coverage beyond traditional medical providers to certain entities organized for the primary purpose of maintaining medical information. (Stats. 1993, ch. 1004, § 1, p. 5693.) In 1999, the Legislature added section 56.101, which requires providers of health care to preserve the confidentiality of medical information and allows individuals to recover damages if their confidential information is negligently released. (Stats. 1999, ch. 526, § 3, p. 3647.) Further amendments in 2007 expanded the definition of a "provider of health care" under section 56.06, subdivision (a) to include businesses that maintain personal health records — i.e. companies that enable consumers to store their health information so that they can manage their own records. (Stats. 2007, ch. 699, § 1, p. 5904.) And in 2013, the Legislature added section 56.06, subdivision (b), defining businesses that offer medical information maintenance software or hardware to consumers as "providers of health care," with companies offering mobile applications to manage medical records as a prime example. (Stats. 2013, ch. 296, § 1.)

Illuminate challenges the Court of Appeal's holding that J.M. has adequately stated a cause of action under sections 56.10 and 56.101 of the CMIA. "We review de novo questions of statutory construction. In doing so, ' "our fundamental task is to 'ascertain the intent of the lawmakers so as to effectuate the purpose of the statute.' " ' [Citation.] As always, we start with the language of the statute, 'giv[ing] the

words their usual and ordinary meaning [citation], while construing them in light of the statute as a whole and the statute's purpose [citation].' " (*Apple Inc. v. Superior Court* (2013) 56 Cal.4th 128, 135.)

A.

Because sections 56.10 and 56.101 govern "provider[s] of health care," we first address whether Illuminate is a "provider of health care" under subdivision (a) or (b) of section 56.06.

Section 56.06, subdivision (a) defines "provider of health care" to mean "[a]ny business organized for the purpose of maintaining medical information *in order to make the information available to an individual or to a provider of health care at the request of the individual or a provider of health care, for purposes of allowing the individual to manage the individual's information, or for the diagnosis and treatment of the individual*." (Italics added.)

Setting aside whether Illuminate is a "business organized for the purpose of maintaining medical information" (§ 56.06, subd. (a)), we discern two types of requirements in the italicized language. First, a covered business is one that maintains medical information "in order to make the information available to an individual or to a provider of health care at the request of the individual or a provider of health care." (*Ibid.*) Second, a covered business is one that makes medical information available to an individual or a provider of health care upon request for one of two purposes: to "allow[] the individual to manage the individual's information, or for the diagnosis and treatment of the individual." (*Ibid.*)

J.M.'s complaint alleges that Illuminate makes its tools and data available to "educators," in addition to "parents" and

"students," in order to help them assess students' educational needs, monitor students' progress, and provide appropriate educational services. J.M. does not allege that the Ventura County Office of Education or any of its teachers or officials is a provider of health care. (Cf. § 56.05, subd. (p).) Nor does he allege that Illuminate makes medical information available to individuals in order to allow them to manage their information or that Illuminate provides medical information to health care providers or individuals for diagnosis and treatment of an individual.

The Court of Appeal said "Illuminate uses student medical information and 'the diagnosis and treatment plans of children' to 'diagnose students' needs' and monitor their progress." (*Illuminate*, *supra*, 103 Cal.App.5th at p. 1131.) J.M. highlights the allegation that Illuminate "provides 'educators with the right dyslexia screening data' because 'educators need the right data about students' early reading skills to identify if they are exhibiting deficits associated with dyslexia.' With its 'dyslexia screening, progress monitoring, and aligned interventions, students can make significant reading improvements.' " But these allegations do not bring Illuminate within the ambit of section 56.06, subdivision (a). The Legislature has made clear that when school districts screen students for risk of reading difficulties, including dyslexia, "[s]creening results shall be used as a flag for potential risk of reading difficulties, not as a diagnosis of a disability." (Ed. Code, § 53008, subd. (*l*).) While J.M. alleges that Illuminate uses students' medical information, including diagnosis and treatment plans, to help educators assess and meet students' educational needs, he does not allege that Illuminate makes such information available to any health care provider or individual for the diagnosis of an individual.

Nor does he allege that Illuminate makes dyslexia screening data or any other medical information available to an individual so that the individual can manage the information.

The Attorney General highlights J.M.'s allegation that Illuminate's internet platforms store student data "with access provided to educators, *students and parents* as an aid to educational evaluation, monitoring of progress, and determining an educational plan." But this allegation — which is the only reference in the second amended complaint to students and parents, as opposed to educators, having access to data stored by Illuminate — does not clearly indicate that Illuminate maintains medical information in order to make it available to an individual at the individual's request for a statutorily specified purpose. The alleged "access provided" is qualified by the purpose of "aid[ing] . . . educational evaluation, monitoring of progress, and determining an educational plan." That purpose does not necessarily align with a purpose of allowing medical information management by an individual or enabling diagnosis of an individual. The complaint does not indicate, for example, whether students and parents have access to students' medical information for noneducational purposes, or whether the internet platforms enable students and parents to download the information for their own use or to access the information whenever they wish. The complaint's bare mention of "access provided . . . to students and parents" is insufficient to bring Illuminate within the coverage of section 56.06, subdivision (a).

J.M. also argues that Illuminate qualifies as a "provider of health care" under section 56.06, subdivision (b), which includes "[a]ny business that offers software or hardware to consumers, including a mobile application or other related device that is

designed to maintain medical information in order to make the information available to an individual or a provider of health care at the request of the individual or a provider of health care, for purposes of allowing the individual to manage the individual's information, or for the diagnosis, treatment, or management of a medical condition of the individual." For reasons already stated, J.M. has not sufficiently alleged that Illuminate's internet platforms make medical information available to students and parents at their request for a statutorily specified purpose. Apart from a sole reference to "access provided . . . to students and parents," the entirety of J.M.'s allegations about Illuminate's services focus on its provision of "educational software applications and technology support to the school districts" that are its customers, in order to aid student assessment and educational planning.

Our reading of subdivisions (a) and (b) of section 56.06 is supported by the legislative history. Section 56.06 was added in 1993 to "authorize medical information corporations to gather and collect medical information" so that they can "disseminate this information to patients and health care providers at their request." (Sen. Floor Analysis, 3d reading analysis of Assem. Bill No. 336 (1993–1994 Reg. Sess.) as amended July 2, 1993, p. 2.) The Legislature passed the bill with support from the Medic Alert Corporation, which had sought statutory authorization for its medical information-sharing service. (*Ibid.*) The service enabled subscribers to share their medical information to "aid providers of health care in timely and accurate diagnosis of conditions afflicting subscribers in emergency situations where the subscriber may be incoherent, comatose or lack recall." (*Ibid.*) As noted, J.M. alleges that Illuminate makes medical information available to educators,

students, and parents to aid educational planning; he has not alleged that Illuminate makes medical information available to health care providers or individuals for the purpose of diagnosing a medical condition.

Also instructive are the 2007 amendments to section 56.06, subdivision (a), which expanded the definition of "provider of health care" and added to the purpose requirement. (Stats. 2007, ch. 699, § 1, p. 5904.) These changes extended the CMIA's coverage to "companies that maintain personal health records," meaning companies that allow individuals to "enter their medical information on a website and build their own electronic medical records." (Assem. Com. on Judiciary, Analysis of Assem. Bill No. 1298 (2007–2008 Reg. Sess.) as introduced Feb. 23, 2007, pp. 1, 4.) Such companies enable individuals to "send the records to medical providers and have ready access to that information whenever it is needed," thereby providing a "central repository for a person's health records." (*Id.* at p. 4.) The Legislature highlighted WebMD's personal health record storage functionality and a statement from a Google Vice President that such businesses will make it easier for individuals to control their health care data. (See Sen. Com. on Judiciary, Analysis of Assem. Bill No. 1298 (2007–2008 Reg. Sess.) as amended June 14, 2007, pp. 10–11.) While such entities are not the only ones covered by the statute, J.M. has not alleged that Illuminate is a personal health records company, that its services allow individuals to build their own medical records, or that its internet platforms serve as a repository of students' personal health records and allow them to access and share those records as they please. Rather, J.M. alleges that Illuminate stores medical information in order to

help educators evaluate, monitor, and address students' educational needs.

The Court of Appeal said the 2013 amendments adding section 56.06, subdivision (b) to the CMIA were designed to ensure that the CMIA applied to all " 'vendors that maintain medical information . . . whether or not the business was organized for that purpose.' " (*Illuminate*, *supra*, 103 Cal.App.5th at p. 1132.) But the legislative history explains that the amendments sought to ensure that "businesses that offer personal health care records, whether online or through a mobile application, are subject to CMIA requirements," as personal health record services were "increasingly offered through mobile applications, potentially raising a new set of privacy concerns." (Assem. Com. on Judiciary, Analysis of Assem. Bill No. 658 (2013–2014 Reg. Sess.) as introduced Feb. 21, 2013, p. 1.) According to the bill's author, before this amendment, the CMIA did not cover personal health records services offered by independent commercial vendors; it covered only such services provided by physicians or health plans. (Sen. Com. on Judiciary, Analysis of Assem. Bill No. 658 (2013–2014 Reg. Sess.) as amended Apr. 22, 2013, pp. 3–4.) The legislative history further notes that the 2013 amendments cover personal health records services that "keep track of such things as how [an individual's] medications are affecting them, or how they're feeling from day to day." (Office of Assemblymember Ian C. Calderon, Fact Sheet, Assem. Bill No. 658 (2013–2014 Reg. Sess.), p. 1.) It specifically mentioned "[d]iabetics" who "may use a [personal health record] to record their glucose levels" or "[p]eople with hypertension" who "may want to use [a personal health record] to track their blood pressure readings." (*Ibid.*) J.M.'s allegations do not establish that Illuminate is a vendor of

personal health records services or that it offers consumer services of the kind that the Legislature intended to cover.

We do not suggest that an entity must be one described in the legislative history to be covered by the CMIA. Section 56.06 was written broadly with the understanding that internet platforms are quickly evolving and that platforms other than the examples cited may align with the purpose requirements in the statute. At the same time, we note that although the CMIA was designed to adapt to technological changes in the way medical information is stored and used, its scope has limits. This is reflected in the Legislature's decision to include a specific definition of "providers of health care" that does not sweep within its ambit *any* entity that stores medical information.

B.

The Court of Appeal also concluded that Illuminate faces liability because the CMIA "applies to '[a] recipient of medical information' (§ 56.13) and to a 'provider of health care, health care service plan, pharmaceutical company, contractor, *or any other entity*' that seeks an authorization for 'disclosure of protected health information.' (§ 56.11, subd. (c), italics added.)" (*Illuminate*, *supra*, 103 Cal.App.5th at p. 1132.) But J.M. does not allege that Illuminate is a covered entity under section 56.11, subdivision (c), so that provision has no bearing on his CMIA claim. And we do not address whether Illuminate is a " '[c]ontractor' " under section 56.05, subdivision (d) because J.M. does not develop that claim here.

J.M. does allege that Illuminate is covered by section 56.13, which says: "A recipient of medical information pursuant to an authorization as provided by this chapter or pursuant to the provisions of subdivision (c) of Section 56.10

may not further disclose that medical information except in accordance with a new authorization that meets the requirements of Section 56.11, or as specifically required or permitted by other provisions of this chapter or by law." Putting aside whether Illuminate "disclose[d]" information by suffering a data breach, J.M. has not alleged that Illuminate received "medical information pursuant to an authorization as provided by this chapter or pursuant to the provisions of subdivision (c) of Section 56.10." (§ 56.13.) J.M.'s pleadings do not mention any authorization by which Illuminate received his medical information. (See §§ 56.05, subd. (a) [" 'Authorization' means permission granted in accordance with Section 56.11 or 56.21 for the disclosure of medical information."], 56.11 [setting forth requirements obtaining medical information from a patient], 56.21 [setting forth requirements for a patient's "employer" to disclose medical information].) Nor does J.M. allege that Illuminate received his information pursuant to any provision of section 56.10, subdivision (c). In short, J.M. has not sufficiently alleged that Illuminate is covered by section 56.13.

C.

Illuminate also argues that the Court of Appeal erred in concluding that J.M. has shown sufficient injury to state a claim under the CMIA. According to Illuminate, a plaintiff must allege his or her medical records were actually viewed by an unauthorized person in order to state a cognizable injury under the CMIA. The Court of Appeal implicitly disagreed: "The Legislature intended to create a cause of action for 'negligent storage' leading to the 'unauthorized "access" ' of medical information. . . . Here there is an allegation that there was an agreement to safeguard this information, Illuminate breached it, and it was also negligent. It also failed to promptly notify the

victims of the data breach for five months. [¶] The allegations demonstrate the type of harm the Legislature sought to prevent in enacting the CMIA-negligence causing a data breach that exposed confidential information to cyber hackers. . . . They support 'a credible threat of real and immediate harm' as a result of the data breach." (*Illuminate*, *supra*, 103 Cal.App.5th at p. 1133, citations omitted.)

Section 56.101, subdivision (a) requires a covered entity "who creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information [to] do so in a manner that preserves the confidentiality of the information contained therein." A covered entity "who negligently creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information shall be subject to the remedies and penalties provided under subdivisions (b) and (c) of Section 56.36." (*Ibid.*) Section 56.36, subdivision (b) provides a cause of action for violations of section 56.101 for individuals whose confidential information was "negligently released." Notably, section 56.36, subdivision (b)(1) provides for "nominal damages" of $1,000 and says "it is not necessary that the plaintiff suffered or was threatened with actual damages."

Illuminate's position — that no CMIA liability exists unless a plaintiff's medical information was actually viewed by an unauthorized party — has its origins in Court of Appeal decisions beginning with *Regents of the University of California v. Superior Court* (2013) 220 Cal.App.4th 549 (*Regents*). In that case, a university physician took home an encrypted external hard drive with patients' medical records and "left it unsecured with the encryption password." (*Id.* at p. 554.) A thief stole the hard drive during a home invasion robbery, and the plaintiff sued the university on behalf of 16,000 patients whose medical

information was on the hard drive, seeking nominal damages of $1,000 for each class member. (*Id.* at pp. 554–555 & fn. 3.) On demurrer, the Court of Appeal said that a plaintiff filing suit under section 56.36, subdivision (b) must "plead[], and ultimately prov[e], that the confidential nature of the plaintiff's medical information was breached as a result of the health care provider's negligence." (*Id.* at p. 570.) Because "no one (except perhaps the thief) knows what happened to the [stolen hard drive], [the plaintiff] cannot allege her medical records were, in fact, viewed by an unauthorized individual." (*Ibid.*) According to the court, the Legislature intended a CMIA violation to require "more than an allegation of loss of possession by the health care provider." (*Regents*, at p. 570; see *id.* at p. 554 [sustaining demurrer because the plaintiff "cannot allege her information was improperly viewed or otherwise accessed"].)

The Court of Appeal in *Sutter Health v. Superior Court* (2014) 227 Cal.App.4th 1546 (*Sutter Health*) employed similar reasoning. The plaintiffs alleged violations of sections 56.10 and 56.101 after a desktop computer containing their medical records was stolen from a Sutter Health office. (*Sutter Health*, at pp. 1551, 1552.) On demurrer, the Court of Appeal said the "mere possession of the medical information or records by an unauthorized person was insufficient to establish breach of confidentiality if the unauthorized person has not viewed the information or records." (*Id.* at p. 1553.) The court reasoned that section 56.101, subdivision (a) allows for a change or even loss of possession of medical information "as long as confidentiality is preserved." (*Sutter Health*, at p. 1556.) Although a "change of possession increase[s] the risk of a confidentiality breach," the statute "does not provide for liability for increasing the risk of a confidentiality breach. It provides

for liability for failing to 'preserve[] the confidentiality' of the medical records. (§ 56.101, subd. (a).)" (*Id.* at p. 1557.) "No breach of confidentiality takes place until an unauthorized person views the medical information." (*Ibid.*; accord, *Vigil v. Muir Medical Group IPA, Inc.* (2022) 84 Cal.App.5th 197, 213–218 (*Vigil*) [agreeing with *Sutter Health* and applying the "actually viewed" rule to a case where a former medical group employee improperly downloaded personal information for over 5,400 patients].)

Although we express no view on the outcomes in *Regents* and *Sutter Health*, we reject the rule that no breach of confidentiality has occurred until medical information is actually viewed by an unauthorized person. Further, we agree with the Attorney General that "the key criterion in determining whether a confidant has failed to preserve the confidentiality of information is whether the information is exposed to a significant risk of unauthorized access or use."

Section 56.101, subdivision (a) requires covered entities to "preserve[] the confidentiality" of medical information. In ordinary usage, "confidentiality" requires keeping information private or secret. When confidential information is made public or exposed to an unauthorized party, confidentiality is compromised whether or not anyone actually views it. This interpretation is bolstered by reading section 56.101 together with section 56.36, subdivision (b), which authorizes a cause of action for negligent release of confidential medical information. As noted, the latter provision says "it is not necessary that the plaintiff suffered or was threatened with actual damages" in order to recover nominal damages of $1,000 for a violation. (§ 56.36, subd. (b)(1).) The Legislature's inclusion of a "nominal" remedy for persons who were not actually damaged or even

threatened with actual damages signals that liability under the statute focuses on the allegedly negligent conduct of the covered entity, not on the resulting harm to the plaintiff. A rule that no liability exists unless negligently released medical information is actually viewed by an unauthorized party is difficult to square with the Legislature's authorization of recovery for a plaintiff who has not even been "threatened with actual damages." (*Ibid.*)

The court in *Vigil* "agree[d] with *Sutter Health*'s reasoning that section 56.101, subdivision (a), which allows a health care provider to 'dispose' of or 'abandon' medical information so long as the confidentiality of that information is preserved, indicates the Legislature did not intend to 'impose[] liability if the health care provider simply loses possession of the medical records.' (*Sutter Health*, *supra*, 227 Cal.App.4th at p. 1556.)" (*Vigil*, *supra*, 84 Cal.App.5th at p. 213.) But section 56.101, subdivision (a)'s use of the terms "dispose" or "abandon" does not support the view that loss of possession is insufficient for liability when the loss is due to negligence. The statute directs any covered entity "who creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information" to "do so in a manner that preserves the confidentiality of the information." (*Ibid.*) And it penalizes any covered entity "who negligently creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information." (*Ibid.*) The statute simply indicates that non-negligent disposal or abandonment of medical information does not give rise to liability. It does not suggest a general rule that loss of possession is insufficient to establish breach of confidentiality in the case of negligence.

That said, we do not hold that mere loss of possession due to negligence is always sufficient to establish breach of confidentiality. The court in *Sutter Health* worried that in a scenario where "a thief grabbed a computer containing medical information on four million patients, but the thief destroyed the electronic records to reformat and wipe clean the hard drive and sell the computer without ever viewing the information or even knowing it was on the hard drive, the health care provider would still be liable, at least potentially, for $4 billion." (*Sutter Health*, *supra*, 227 Cal.App.4th at p. 1558.) In such a case, it does seem questionable whether liability of that scale comports with the Legislature's intent.

Meanwhile, an "actually viewed" standard would pose difficult problems of pleading and proof. Victims of data breaches are unlikely to know what an unauthorized party has done with their data unless they suffer actual damage (but see § 56.36, subd. (b)(1) [no actual or threatened damage required to recover nominal damages]), and relevant information about the breach may often be in the possession of the covered entity. Moreover, given evolving technologies, data breaches resulting in unauthorized use of medical information may be facilitated by artificial intelligence or automated cybercrime, without anyone actually viewing the information. The difficulty of pleading or proving actual viewing in many data breach scenarios suggests that such a standard may significantly enervate the CMIA, a remedial statute. (See *Pulliam v. HNL Automotive Inc.* (2022) 13 Cal.5th 127, 137 ["We ' "must construe [remedial provisions] broadly, not . . . restrictively" ' [citation] ' "so as to afford all the relief" that their "language . . . indicates . . . the Legislature intended to grant" ' "].)

In light of these competing concerns, we agree with the Attorney General that the primary inquiry with regard to breach of confidentiality is whether the information is exposed to a significant risk of unauthorized access or use. This standard is sufficiently flexible to distinguish between "smash-and-grab hardware theft," where the unauthorized party seeks the hardware and not the data it contains, and conventional data breaches, where the unauthorized party is targeting the data for illicit use. It also provides a suitable standard for evaluating whether other negligent releases of medical information (e.g., an inadvertent public posting, an errant e-mail, an accidentally leaked password) result in a breach of confidentiality. Circumstances potentially relevant to whether information is exposed to a significant risk of unauthorized access or use include the form, duration, and extent of the data breach, as well as any mitigation efforts by the covered entity. Loss of possession of the information is a relevant factor, but it is neither necessary nor always sufficient by itself to establish breach of confidentiality. All relevant circumstances must be considered.

We disapprove *Regents of the University of California v. Superior Court*, *supra*, 220 Cal.App.4th 549, *Sutter Health v. Superior Court*, *supra*, 227 Cal.App.4th 1546, and *Vigil v. Muir Medical Group IPA, Inc.*, *supra*, 84 Cal.App.5th 197, to the extent they are inconsistent with this opinion.

III.

J.M. also alleges a cause of action under the CRA, which sets forth requirements for persons or businesses that maintain computerized data. The statute required certain persons or businesses that own or license "data that includes personal

information" to "disclose a breach of . . . security" "in the most expedient time possible and without unreasonable delay." (§ 1798.82, former subd. (a)(1).) "Any customer injured by a violation of [the CRA] may institute a civil action to recover damages." (§ 1798.84, subd. (b).)

To bring suit under the CRA, "a plaintiff must meet the terms of [section 1798.84] — i.e., he or she must be a 'customer' who has been 'injured by a violation of this title.' " (*Boorstein v. CBS Interactive, Inc.* (2013) 222 Cal.App.4th 456, 467.) The CRA defines a customer as "an individual who provides personal information to a business for the purpose of purchasing or leasing a product or obtaining a service from the business." (§ 1798.80, subd. (c).)

J.M. has not alleged he has a customer relationship with Illuminate under the terms of the CRA. The Ventura County Office of Education, not J.M., purchased Illuminate's services and provided Illuminate with student information. And Illuminate's services help schools and educators monitor student progress and develop appropriate educational interventions. J.M. has not alleged that he "provide[d] personal information to [Illuminate] for the purpose of purchasing or leasing a product or obtaining a service from [Illuminate]." (§ 1798.80, subd. (c).) His complaint contains no allegation that he sought to purchase or lease anything from Illuminate and, fairly read, suggests he provided personal information to the school district, which Illuminate collected and stored, in order to obtain educational services from the school district.

Echoing the Court of Appeal, J.M. argues that "he was an intended beneficiary under the CRA" because, as a student of the school district contracting with Illuminate, he was among

Illuminate's "ultimate 'customers,' consumers, and beneficiaries of its educational services." (*Illuminate*, *supra*, 103 Cal.App.5th at p. 1135.) But the CRA does not authorize suit by all consumers or beneficiaries; it authorizes a civil action for an injured "customer." (§ 1798.84, subd. (b).) Moreover, while the CRA defines an " '[i]ndividual' " in section 1798.80, subdivision (d) as "a natural person," it more narrowly authorizes a lawsuit only by a "customer" who has been injured. (§ 1798.84, subd. (b).)

The limitation of civil actions to an injured "customer" stands in contrast to the CRA's use of broader terms to define the scope of various requirements. (Compare § 1798.83, subd. (a) [addressing businesses with "an established business relationship with a customer"] with §§ 1798.82 [addressing the data of "individuals"], 1798.81.5, subd. (a) [addressing the data of "California residents"].) Moreover, having defined the terms "customer" in the CRA (§ 1798.80, subd. (c)) and "consumer" in the California Consumer Privacy Act of 2018 (§ 1798.140, subd. (i) [defining " '[c]onsumer' " to mean "a natural person who is a California resident"]), the Legislature chose to use the term "customer," not "consumer," in section 1798.84, subdivision (b). We presume the Legislature's choice was deliberate. (See *Ferra v. Loews Hollywood Hotel, LLC* (2021) 11 Cal.5th 858, 866 [courts presume the Legislature intends different words to have different meanings].) Further, there are other laws that permit California residents to bring claims for data privacy violations. (See California Consumer Privacy Act; § 1798.100 et seq. [allowing consumers to enforce protections similar to those in the CRA].)

Because J.M. has not alleged he is a customer of Illuminate within the meaning of the CRA, his complaint does not state a cause of action under that statute.

CONCLUSION

We reverse the judgment of the Court of Appeal and remand this matter to the Court of Appeal for further proceedings consistent with our opinion. We leave it to the courts below to consider whether, in light of our holdings today, J.M. may be granted leave to amend his complaint if he so requests.

LIU, J.

We Concur:

GUERRERO, C. J.
CORRIGAN, J.
KRUGER, J.
GROBAN, J.
EVANS, J.
BUCHANAN, J.*

---

* Associate Justice of the Court of Appeal, Fourth Appellate District, Division One, assigned by the Chief Justice pursuant to article VI, section 6 of the California Constitution.

J.M. v. ILLUMINATE EDUCATION, INC.

S286699

Concurring Opinion by Justice Groban

I agree with the majority's holdings that (1) J.M. has not stated a valid claim under Civil Code sections 56.10, subdivision (a) and 56.101 subdivision (a) of the Confidentiality of Medical Information Act (CMIA) (Civ. Code, § 56 et seq.) because he has not sufficiently alleged that Illuminate Education, Inc. (Illuminate), is a "provider of health care" within the meaning of that act under Civil Code section 56.06, subdivision (a);[1] (2) a plaintiff need not allege that confidential medical information was "actually viewed" by an unauthorized third party to establish a violation of the CMIA under section 56.101, subdivision (a); and (3) J.M. has not adequately alleged a violation of the Customer Records Act (CRA) (§ 1798.80 et seq.) because he was not Illuminate's "customer" within the meaning of that act.

I write separately to address issues the majority does not reach and to elaborate on one that it does. First, I believe that an additional reason J.M. cannot establish a violation of the CMIA under section 56.10, subdivision (a) is because he fails to adequately allege a "disclos[ur]e." Second, I agree with the majority that J.M.'s CMIA claims under sections 56.10, subdivision (a) and 56.101 subdivision (a) fail because he has not adequately alleged that Illuminate is a "provider of health care,"

---

[1] All further references are to the Civil Code unless otherwise indicated.

both for the reasons the majority identifies and for an additional reason the majority does not address. Third, because I do not believe there is a reasonable possibility that J.M. will be able to amend his complaint to sufficiently allege that Illuminate is a provider of health care, I would affirm the trial court's decision to sustain Illuminate's demurrer without leave to amend, rather than leaving that determination to the lower courts. Finally, although I agree that a plaintiff need not allege that medical information was "actually viewed" by an unauthorized third party to state a violation of the CMIA under section 56.101, subdivision (a), I write to further clarify my view of the scope of the "significant risk of unauthorized access or use" standard adopted by the majority. (Maj. opn., *ante*, at pp. 20 and 21.) I address each point in turn below.

First, J.M. alleges that Illuminate violated the CMIA under section 56.10, subdivision (a) by "disclos[ing] medical information . . . without first obtaining an authorization." I agree with the trial court that J.M. has not adequately alleged a disclosure within the meaning of this subdivision. Courts have interpreted the word "disclose" in this provision as requiring "an affirmative communicative act" — that is, an intentional disclosure of medical information by the defendant to an unauthorized recipient. (*Sutter Health v. Superior Court* (2014) 227 Cal.App.4th 1546, 1556 (*Sutter Health*); accord, *Regents of University of California v. Superior Court* (2013) 220 Cal.App.4th 549, 564 (*Regents*) [" 'Disclose' . . . is an active verb, denoting . . . an affirmative act of communication"].) In *Sutter Health*, the court found no disclosure where it was undisputed that the computer containing the confidential medical information "was stolen by, not given to, the unauthorized person." (*Sutter Health*, at p. 1556.) The same is

true here: J.M. does not dispute that his medical information was obtained through an unauthorized cyberattack on Illuminate. Accordingly, he has not alleged, and cannot allege, facts sufficient to show that Illuminate disclosed his information in violation of section 56.10, subdivision (a).

In addition, J.M. alleges that Illuminate violated a different provision of the CMIA, section 56.101, subdivision (a), which does not require a disclosure but instead requires a showing that the defendant negligently failed to preserve the confidentiality of medical information. Like section 56.10, subdivision (a), however, section 56.101, subdivision (a) applies only if Illuminate is a "provider of health care" as defined in section 56.06, subdivision (a) or (b). I agree with the majority that J.M. has not adequately alleged that Illuminate is a health care provider (maj. opn., *ante*, at p. 4) for the reasons the majority states as well as for an additional reason, and both of his CMIA claims fail as a result.

Section 56.06, subdivision (a) defines "provider of health care" as a business (1) organized for the purpose of maintaining medical information; (2) in order to make the information available to an individual or to a provider of health care; (3) for purposes of allowing the individual to manage the individual's information or for the diagnosis and treatment of the individual. The majority addresses the second and third elements of this definition but does not decide whether J.M. has satisfied the first element — whether Illuminate is organized for the purpose of maintaining medical information. (Maj. opn., *ante*, at p. 8)

I do not believe J.M. has adequately alleged that maintaining medical information is one of Illuminate's organizing purposes. Although I agree with the Attorney

General that such maintenance need not be the business's "central or exclusive" purpose, I also agree that it must nevertheless be "integral to or inseparable from some significant aspect of the business's activity." When asked at oral argument to identify where in the proposed second amended complaint J.M. alleges this element, J.M.'s counsel pointed only to paragraph 21, which states that Illuminate "regularly collects medical information from school districts, including personally identifiable information and medical information, including the diagnosis and treatment plans of children." This bare allegation is insufficient to show that maintaining medical information is integral to Illuminate's alleged business purposes.

J.M. may well attempt to amend his complaint to allege that Illuminate's maintenance of certain medical information — such as dyslexia diagnoses — is integral to its provision of educational services. But even then, under both subdivisions (a) and (b) of section 56.06, J.M. must satisfy the third element of the "provider of health care" definition by alleging that Illuminate makes such information available for the purpose of allowing the individual to manage that information or to diagnose or treat the individual. I agree with the majority that he has not done so. (Maj. opn., *ante*, at pp. 8–14.) J.M. alleges only that Illuminate makes its medical data accessible to educators, students, and parents " 'as an aid to educational evaluation, monitoring of progress, and determining an educational plan' " — not to allow individuals to manage their medical information or to allow health care providers to diagnose or treat the individual. (*Id.* at p. 9.)

J.M. has already attempted to amend his complaint twice and still has been unable to allege facts showing that Illuminate is a provider of health care under the CMIA. At oral argument,

counsel was unable to identify allegations showing that Illuminate maintains medical information for purposes of individual medical information management or for medical diagnosis and treatment, relying instead on allegations stating only that Illuminate collects medical information. This is insufficient. In my view, the trial court properly sustained Illuminate's demurrer without leave to amend.

Finally, I agree with the majority's rejection of the standard adopted by some courts requiring a plaintiff to allege that medical information was "actually viewed" by an unauthorized third party in order to state a violation of the CMIA under section 56.101, subdivision (a). (Maj. opn., *ante,* at p. 19.) I write separately to elaborate on the scope of the "significant risk of unauthorized access or use" standard the majority adopts in its place. Although the majority rejects the "actually viewed" rule, it also correctly explains that "mere loss of possession due to negligence" is insufficient to establish a violation of section 56.101. (Maj. opn., *ante*, at p. 19.) This clarification is important because "if the confidentiality is not breached, the statute is not violated." (*Sutter Health*, *supra*, 227 Cal.App.4th at p. 1556.) The standard the majority adopts in place of the "actually viewed" rule — that a plaintiff must show "a significant risk of unauthorized access or use" (maj. opn., *ante*, at p. 18) — must therefore have some force: It cannot be satisfied by mere speculation or a theoretical possibility of access inherent any time data comes into the possession of an unauthorized third party. Rather, a "significant risk" must be grounded in facts showing that unauthorized access to or use of the data is reasonably likely under the circumstances. Such a risk will not exist where the surrounding facts make access or use unlikely — for example, where stolen data is protected by

robust encryption. That was the case in *Regents*, *supra*, 220 Cal.App.4th 549, where a thief stole an encrypted external hard drive during a home invasion. Because the data was unlikely to be accessed or used, there was no significant risk of unauthorized access or use, and the court properly concluded that the plaintiffs failed to state a claim under section 56.101, even if it articulated the legal standard imprecisely.

For these reasons, I concur in the majority's judgment but would go further by concluding that J.M. has not demonstrated a reasonable possibility of curing the defects in his complaint. I also underscore that the "significant risk of unauthorized access or use" standard requires more than the mere possibility of exposure; it demands allegations showing a realistic and appreciable risk that confidential information will in fact be accessed or misused.

GROBAN, J.

See next page for addresses and telephone numbers for counsel who argued in Supreme Court.

Name of Opinion J.M. v. Illuminate Education, Inc.

Procedural Posture (see XX below)
Original Appeal
Original Proceeding
Review Granted (published) XX 103 Cal.App.5th 1125
Review Granted (unpublished)
Rehearing Granted

Opinion No. S286699
Date Filed: May 14, 2026

Court: Superior
County: Ventura
Judge: Benjamin F. Coats

Counsel:

Potter Handy, Mark D. Potter and James M. Treglio for Plaintiff and Appellant.

Rob Bonta, Attorney General, Nicklas A. Akers, Assistant Attorney General, Michele Van Gelderen and Hunter Landerholm, Deputy Attorneys General, for the California Attorney General as Amicus Curiae on behalf of Plaintiff and Appellant.

Kirkland & Ellis, Devin S. Anderson, Cynthia D. Love, David R. Williams, Mark C. Gillespie and Tammy A. Tsoumas for Defendant and Respondent.

Counsel who argued in Supreme Court (not intended for publication with opinion):

James M. Treglio
Potter Handy LLP
100 Pine Street, Suite 1250
San Francisco, CA 94111
(415) 534-1911

Devin S. Anderson
Kirkland & Ellis LLP
95 South State Street, Suite 2000
Salt Lake City, UT 84111
(801) 877-8115