SUMMER 2026 VOLUME XXVIII, ISSUE 3

CALIFORNIA HEALTH LAW NEWS

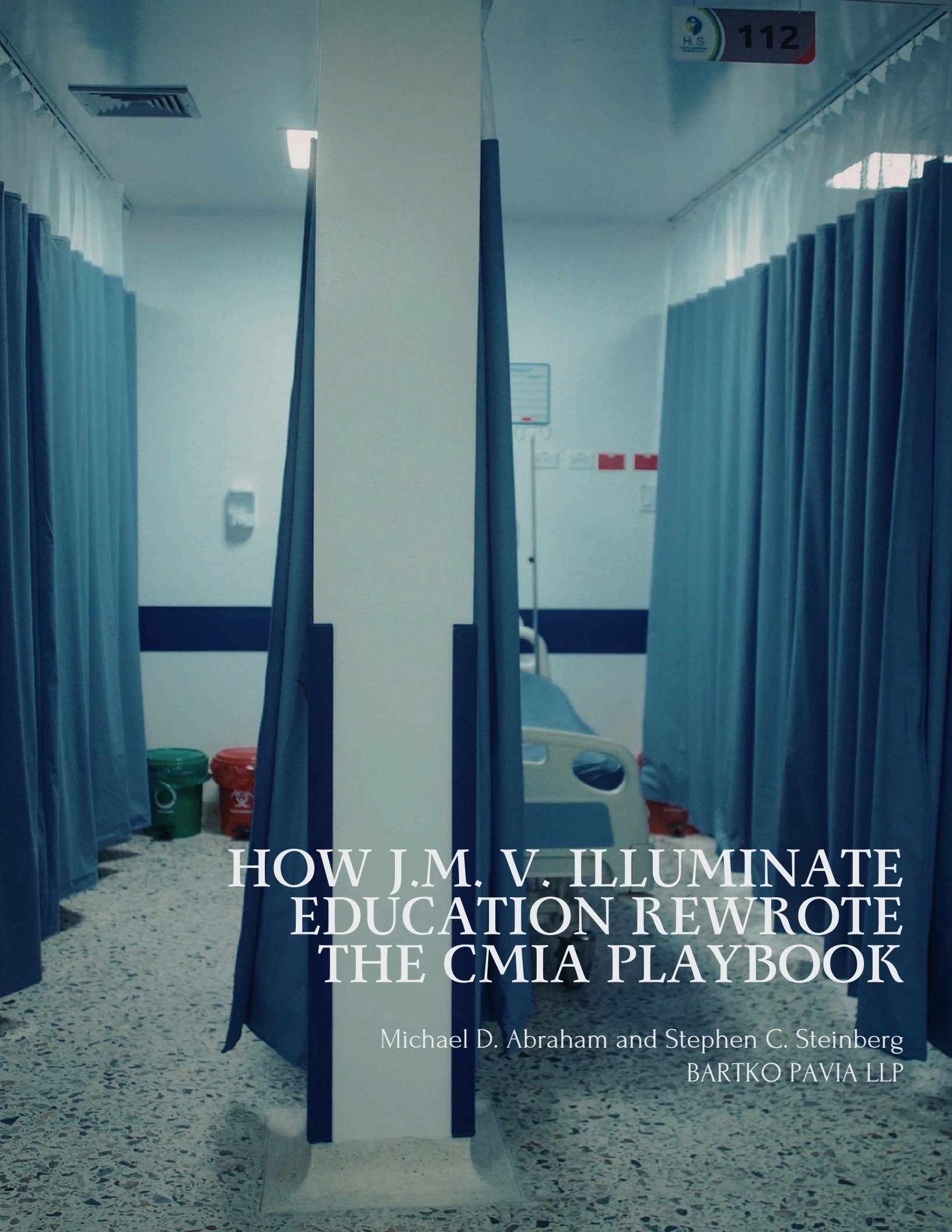
THE LATEST DEVELOPMENTS IN CALIFORNIA HEALTH LAW

How J.M. v. Illuminate Education Rewrote the CMIA Playbook

From Landlines to Health Apps: California Courts Grapple with CIPA's Modern Application

Artificial Intelligence: Through the Lens of a California Physician and Informaticist

Pomona Valley Hospital v. Kaiser: California Court Publishes Guidance on the Reasonable Value of Out-of-Network Emergency Services



HOW J.M. V. ILLUMINATE EDUCATION REWROTE THE CMIA PLAYBOOK

Michael D. Abraham and Stephen C. Steinberg
BARTKO PAVIA LLP

I. Introduction — Why Illuminate Matters to Every Health Care System and Provider

For over a decade, claims under the California Confidentiality of Medical Information Act ("CMIA") typically did not proceed past a pleading challenge unless the plaintiff pleaded facts that an unauthorized person "actually viewed or accessed" the plaintiff's medical information. On May 14, 2026, the California Supreme Court overturned this pleading standard in J.M. v. Illuminate Education, Inc. [1]

The Illuminate decision involved a defendant who was an education technology company, not a health care system or provider. This distinction proved critical. The California Supreme Court first held the defendant was not covered by CMIA. The Court narrowed CMIA's reach to businesses whose primary purpose is maintaining medical information so individuals can manage the information or providers can use the information for diagnosis and treatment—not entities holding medical information that is incidental to other primary functions.

Rather than stop there, the Court also replaced the "actually viewed or accessed" CMIA pleading standard with a requirement that a plaintiff need only plead the defendant's negligence created a "significant risk" of a confidentiality breach. The Court held that the form, duration, and extent of the data breach, as well as any mitigation efforts, should be considered by the trial court in determining if a significant risk had been pleaded, and that loss of possession of the medical information is neither necessary nor sufficient by itself to establish a "significant risk." This holding significantly expands pleading-stage exposure for entities covered by CMIA.

Three issues will shape future CMIA litigation. First, in the context of the specific circumstances at issue, the determination of the scope of the defendant's duty, including whether a particular security measure or action was required.

Second, if the defendant's scope of duty required a particular security measure or action, but it was not implemented, what non-speculative evidence is sufficient to meet the plaintiff's evidentiary burden on causation to be entitled to recover CMIA statutory "nominal" damages or actual damages?

Third, how does the new "significant risk" pleading standard impact the issue of class certification, including whether it gives rise to a predominance of individualized issues?

II. CMIA and Its Legislatively Intended Balance

A. CMIA Overview

1.Structure. CMIA protects "individually identifiable medical information obtained from a patient by a health care provider," subject to "limited circumstances in which the release of such information … is permissible." [2] Two primary prohibitions exist: (a) Section 56.10 bars a covered defendant from disclosing medical information

without authorization, with a breach causing exposure to Section 56.35 remedies; and (b) Section 56.101 requires a covered defendant that "creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information [to] do so in a manner that preserves the confidentiality of the information," with a negligent release causing exposure to Section 56.36's remedies. Both reach only "covered" entities, including a "provider of health care" or "contractor" as defined in Sections 56.05 and 56.06, including businesses that maintain medical information for the primary purpose of managing the information or treatment.

2.Statutory Remedies for Private Plaintiffs (Sections 56.35 and 56.36). Section 56.35 provides a patient whose medical information has been used or disclosed in violation of Sections 56.10, 56.104, 56.107, 56.20, or 56.26(a), and who has sustained economic loss or personal injury therefrom, with legal remedies consisting of compensatory damages, punitive damages up to $3,000, attorney's fees up to $1,000, and costs.

Section 56.36(b) supplies an individual with legal remedies for negligently released medical information consisting of statutory "nominal damages" of $1,000 for which "it is not necessary that the plaintiff suffered or was threatened with actual damages," and actual damages. CMIA's statutory "nominal" damages are the primary driver of class litigation. Multiplied across a breached large database or website or patient portal, they can create exposure in the millions or even billions of dollars.

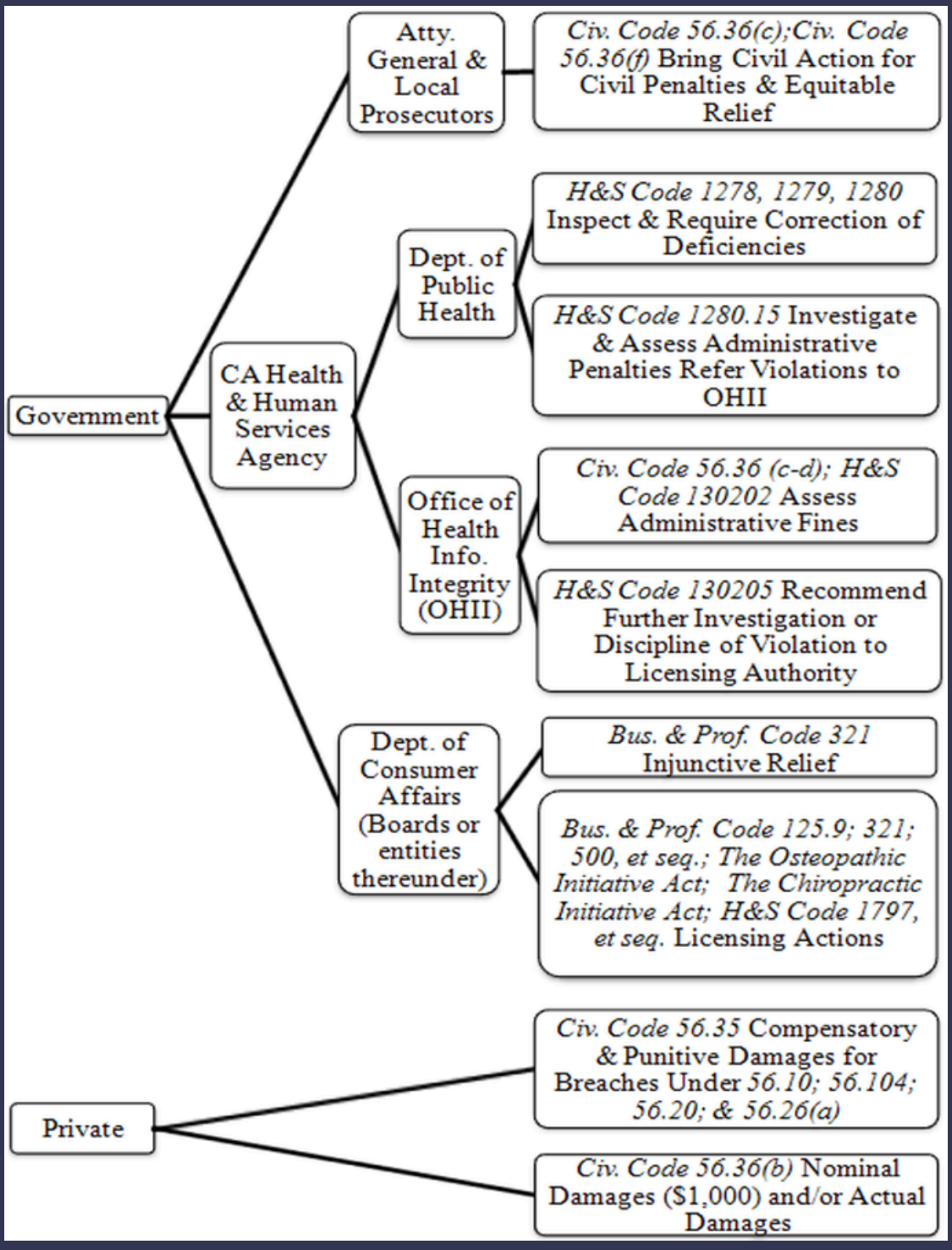
As distinct from the legal remedies provided to private plaintiffs in Sections 56.35 and 56.36(b), Sections 56.36(c) and (f) provide for administrative fines and for civil penalties in an action by public enforcers.

B. The Legislature Originally Enacted Regulatory Enforcement To Address Risk And a Limited Private Right of Action For An Actual Breach of Confidentiality

CMIA is one part of a larger integrated scheme. State regulatory agencies have enforcement powers to address risk-based standards under CMIA (Civil Code § 56.36(c), (f)), and Cal. Health & Safety Code §§ 1280.15(a),(i),(j)(2) and 130202-130203). Additionally, federal and state public prosecutors and agencies have enforcement powers to address risk under the federal Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191, 110 Stat. 1936; 45 C.F.R. §§ 160.101-160.104, 160.201-160.205, 164.102-164.106, 164.302-164.318 [security requirements]; and the Health Information Technology for Economic and Clinical Health Act § 13411; and 42 U.S.C. § 17940 [compliance audits].

CMIA's private right of action is one component of this integrated scheme, not its centerpiece. Unlike regulatory agencies and public enforcers, private plaintiffs are limited to legal (not equitable) relief for intentional disclosure or negligent handling of medical information. [3]

The following diagram reflects these integrated statutory provisions and the Legislature's balance for protection of confidential medical information:



In Illuminate, unlike in the earlier Court of Appeal decisions that gave rise to the "actually viewed or accessed" standard—Sutter Health v. Superior Court [4] and Regents of the University of California v. Superior Court [5]—the Legislature's balance as reflected by this integrated scheme was not presented to the Supreme Court, which may partially explain the differing outcome.

C. CMIA Appellate Case Law Before Illuminate: The "Actually Viewed" Trilogy

In Regents of the University of California v. Superior Court [6], a physician took an encrypted hard drive with 16,000+ patients' records and an index card with the password, which were stolen from his hotel in Hawaii. The Second District issued a writ directing that a demurrer be sustained without leave to amend, holding that a plaintiff must plead and prove "more than an allegation of loss of possession" under CMIA. The plaintiff must also plead and prove the "confidential nature" of the plaintiff's medical information was actually breached, meaning the records were improperly viewed or accessed.

In Sutter Health v. Superior Court [7], a computer with password-protected records of 4,000,000+ patients was stolen from an office. The plaintiffs could not plead what, if anything, had happened to the medical information on the computer. The Third District issued a writ directing that a demurrer be sustained without leave to amend, holding that "[n]o breach of confidentiality takes place until an unauthorized person views the medical information." In so holding, the Court of Appeal considered a thief who wipes and then resells stolen hardware without ever viewing the data, and reasoned that a $4 billion potential liability based on such facts could not have been the Legislature's intent.

In Vigil v. Muir Medical Group IPA, Inc. [8], a departing employee downloaded the information of 5,400+ patients. The First District affirmed denial of class certification, agreed with Sutter Health, and extended the "actually viewed" standard from a pleading requirement to a class certification requirement. Because each class member had to prove their own medical information was improperly viewed—an individualized inquiry subject to cross-examination—individual issues predominated precluding class certification.

This trilogy of cases created a formidable defense.

III. The Illuminate Court of Appeal Decision

Illuminate Education, Inc. runs a nationwide platform that stores and provides access to K-12 student data including, for some, medical information. J.M. gave medical information to his school district, which passed it to Illuminate. After a ransomware data breach, J.M. filed a proposed second amended complaint alleging that his information was stolen and "actually viewed," citing solicitations and "phantom Amazon" calls as the supporting facts. The trial court sustained Illuminate's demurrer without leave to amend, concluding that Illuminate was not a covered entity, and that no actionable "disclosure" or "release" was alleged. The Second District reversed, holding Illuminate was covered by CMIA and J.M. had adequately pleaded a CMIA claim, citing federal cases addressing Article III standing based on risk. [9]

IV. The California Supreme Court Illuminate Decision

A. The Key Holdings, Including a New Pleading Paradigm for Private Actions

The Supreme Court unanimously reversed, with Justice Liu writing for the Court and Justice Groban writing a separate concurrence. As noted above, none of the briefing before the Court presented the integrated statutes of which CMIA is a part nor the Legislature's enacted framework balancing agencies with expertise to enforce privacy and security standards with the limited private right of action for legal remedies under CMIA. Some of the opinion's holdings narrow and some expand CMIA.

1. CMIA-covered entities—the narrowing side. First, the Court held that Illuminate was not adequately alleged to be a "provider of health care" under Section 56.06, which requires that a business be organized, or that software or hardware be designed, for the primary purpose of maintaining medical information to make it available to individuals for their management of the information or to providers for diagnosis and treatment. Illuminate's educational purpose satisfied neither, and allegations about the medical information being used for dyslexia screening did not help because that is, by statute, "a flag for potential risk," "not ... a diagnosis." [10]

2. "Significant risk of unauthorized access or use"—the expanding side. The Court also held that a plaintiff need not allege actual viewing because "confidentiality is breached when the information is exposed to a significant risk of unauthorized access or use." The Court reasoned that the statute "focuses on the ... negligent conduct of the covered entity, not on the resulting harm." Therefore, the "primary inquiry ... is whether the information is exposed to a significant risk of unauthorized access or use," considering "the form, duration, and extent of the ... breach" and "mitigation efforts"; loss of possession is "neither necessary nor always sufficient" to establish breach of confidentiality, and "[a]ll relevant circumstances must be considered." The Court disapproved Regents, Sutter Health, and Vigil "to the extent they are inconsistent with" this opinion, while "express[ing] no view on the outcomes in Regents and Sutter Health." Notably, citing Sutter Health, the Illuminate majority agreed that a class action giving rise to a potential multi-billion dollar recovery based on risk from loss of possession of information alone could not be squared with the Legislature's intent in enacting CMIA.

3. The Groban concurrence—a potential defense roadmap. Justice Groban joined Justice Liu's opinion, but flagged three key points. First, "disclosure" under section 56.10(a) requires "an affirmative communicative act," so stolen data is not "disclosed." Second, the "significant risk" pleading standard "cannot be satisfied by mere speculation or ... theoretical possibility," but "must be grounded in facts showing that unauthorized access to or use of the data is reasonably likely." "Robust encryption" can defeat it, citing Regents. Third, in joining with the majority that "mere loss of possession due to negligence" is insufficient to establish a violation of section 56.101, Justice Groban stated "this clarification is important because "if the

confidentiality is not breached, the statute is not violated," quoting with approval the Sutter Health decision. While made in a decision addressing pleading requirements, this point illustrates the open issue of what is the plaintiff's evidentiary burden of proof. Additionally, while Justice Groban's concurring opinion provides defense arguments for circumstances involving theft or loss of hardware with encrypted data, it does not address other circumstances, including a ransomware attack where the target of the attack paid the hacker for promised deletion of the data.

B. The New Paradigm

Three points deserve emphasis. First, moving the decisive question from a discrete pleaded fact (actual viewing or access of medical information by an unauthorized individual) to an "all relevant circumstances" inquiry will likely push many cases past pleading challenges. This will result in healthcare defendants facing ongoing litigation expenses and exposure often in the context of putative class actions, despite the California Supreme Court in Illuminate and Court of Appeal in Sutter Health holding this is inconsistent with legislative intent. Second, the Court left the bounds of what kind of non-speculative facts may establish "significant risk" for later development. While the concurrence's standard of "facts showing that unauthorized access to or use of the data is reasonably likely" is the natural candidate, the majority did not adopt it nor provide other guidance. Third, the Court answered a pleading question, and the Court did not reach the plaintiff's evidentiary burden on the merits—recognized in Regents and in Justice Groban's concurrence in Illuminate citing Sutter Health—that a plaintiff ultimately must prove an actual breach of confidentiality to be entitled to any recovery since otherwise the statute is not breached.

V. Defense Strategies After Illuminate

A. The Defendant or Data Is Not Within the Scope of CMIA

Section 56.06 is purpose-focused. It is not enough that a business stores medical information. It must maintain the information in order to make it available for a stated purpose: individual management or provider diagnosis or treatment.

Section 56.13 is tied to authorization channels. A defendant is a covered "recipient" only if it receives the medical information pursuant to a CMIA authorization or under Section 56.10(c), so a vendor receiving data outside those channels for reasons other than those covered by Section 56.06 should not be exposed to liability under CMIA.

The Data Is Not "Medical Information" As Defined by CMIA. Not all data held by a covered defendant constitutes "medical information" under CMIA. Pursuant to the governing case law, "the mere fact that a person may have been a patient at the hospital at some time is not sufficient." "Medical information" under CMIA must be "individually identifiable" and "include information relating to medical history, mental or physical condition, or treatment of the individual." [11]

B. No Breach of the Defendant's Duty and/or No Causation

(i) The scope of a defendant's duty. Whether a defendant's duty required a particular security measure or action is an issue of law for the Court to decide. Consideration should be given to having this issue resolved early through summary judgment/adjudication. [12]

(ii) Lack of causation. A plaintiff's burden is not met by speculation or proving "abstract negligence"—that the defendant did not take a security measure or action urged by the plaintiff or expert—without proving a causal connection to an injury to the named plaintiff. [13] For example, an expert's opinion that the defendant should have implemented software security patches more quickly would constitute "abstract negligence" where the underlying incident involved a zero-day exploit (meaning a previously unknown vulnerability for which no patch then existed) or where the named plaintiff's data was already downloaded before a patch was available.

(iii) No actual breach of confidentiality or no "reasonably likely" unauthorized access to or use of the data. Even though plaintiffs do not have to prove threatened or actual damages under CMIA Section 56.36(b) to recover statutory "nominal" damages, and Illuminate replaced the "actually viewed or accessed" with the "significant risk" pleading standard, it is not enough to show mere loss of possession. And at least according to the concurrence, the pleading must be grounded in facts that it is "reasonably likely" their medical information was or will be accessed or used by an unauthorized individual. [14]

For example:

1.Strong encryption. An entity that maintained medical information under HIPAA-compliant encryption at rest and in transit can argue it did not breach the scope of its duty, and independently, no "significant risk" exists in cases not involving loss of the encryption key or hacking of a system with built-in ability to decrypt the medical information.

2.Zero-day vulnerability and/or timely patching. Where a breach exploits a zero-day exploit, or the entity patched a previously unknown vulnerability within a reasonable time from when a patch became available, it met the scope of its duty. Negligence requires an unreasonable failure to guard against a foreseeable and avoidable risk.

C. No Class Certification based on Individual Issues Predominating

The court's class certification analysis includes determining whether common issues predominate over individualized issues. In evaluating this issue, the court considers the substantive legal elements of a CMIA claim and the evidence required to prove such elements. As stated in Justice Groban's concurring opinion, "if the confidentiality is not breached, the statute is not violated." [15] Whether each class member's medical information was improperly accessed or used often requires individual analysis and evidence, thereby making individual issues predominate. Additionally, the unauthorized access or use, if any, must be of a type that constitutes an actual breach of confidentiality.

For example, deleting data off of a stolen computer to get it ready for sale by itself would not constitute access that causes the required actual breach of confidentiality.

VI. Conclusion

Illuminate may have slipped under the radar of many health care systems and providers. It represents a sea change that creates broader exposure at the pleading stage for the traditional health care sector, and a narrower scope of coverage for some medical information data-handling vendors on the periphery. That said, strong defenses to CMIA claims continue to exist.

Endnotes

[1] (2026) 19 Cal.5th 705.
[2] Loder v. City of Glendale (1997) 14 Cal.4th 846, 859.
[3] Civ. Code §§ 56.35 and 56.36(b) ["In addition to any other remedies available at law ..."].
[4] (2014) 227 Cal.App.4th 1546.
[5] (2013) 220 Cal.App.4th 549.
[6] Id.
[7] (2014) 227 Cal.App.4th 1546.
[8] (2022) 84 Cal.App.5th 197.
[9] J.M. v. Illuminate Education, Inc. (2024) 103 Cal.App.5th 1125.
[10] Cal. Ed. Code, § 53008(1).
[11] Eisenhower Med. Ctr. v. Superior Ct. (2014) 226 Cal. App. 4th 430.
[12] See e.g., Kahn v. East Side Union High School Dist. (2003) 31 Cal.4th 990, 1004 ["the question of 'the existence and scope' of the defendant's duty is one of law to be decided by the court, not by a jury, and therefore it generally is 'amenable to resolution by summary judgment.'"].
[13] See e.g., Noble v. Los Angeles Dodgers, Inc. (1985) 168 Cal.App.3d 912, 916; Nola M. v. University of Southern California (1993) 16 Cal. App. 4th 421, 435; Saelzler v. Advanced Group 400 (2001) 25 Ca1.4th 763, 773, 778, 780-781.
[14] Illuminate, 19 Cal.5th at 721, 723.
[15] Illuminate, 19 Cal.5th at 727, quoting Sutter Health, 227 Cal.App.4th at 1556.

Michael Abraham is a partner in the Bartko Pavia LLP law firm. He has over 35 years of litigation experience. Michael's healthcare practice focuses on representing healthcare systems, entities, and providers with respect to litigation involving privacy, website analytics, peer review proceedings, antitrust issues, and commercial disputes. On behalf of healthcare entities, technology companies, Department of Defense contractors, and other clients, Michael has successfully handled a wide range of litigation as well as government investigations. He is an update author for the CEB treatise on Privacy Compliance and Litigation.

Steve Steinberg is a partner in the Bartko Pavia LLP law firm. He has over 20 years of trial and litigation experience focused on privacy including CMIA claims and CIPA claims over alleged wiretapping, pen registers and trap and trace devices, intellectual property including theft of trade secrets and trademark and copyright infringement, cryptocurrency, and other complex business disputes. He has defended healthcare systems, entities, and providers in actions involving privacy and wiretap claims based on website cookies and pixels, civil rights claims, breach of contract, and a wide variety of other claims. Steve has served as an update author for the CEB treatises on Privacy Compliance and Litigation, as well as trademark law.