Filed 9/26/22; certified for publication 10/18/22 (order attached)

IN THE COURT OF APPEAL OF THE STATE OF CALIFORNIA

FIRST APPELLATE DISTRICT

DIVISION TWO

MARIA VIGIL, Plaintiff and Appellant, v. MUIR MEDICAL GROUP IPA, INC., Defendant and Respondent.	A160897 (Contra Costa County Super. Ct. No. C1801331)

Maria Vigil filed a class action against Muir Medical Group IPA, Inc. (Muir), claiming that it failed to secure patients' personal information, thereby allowing a former employee to download private medical information belonging to over 5,000 patients and take it with her when she left her employment with Muir. Among other causes of action, the class complaint alleges that Muir violated Civil Code[1] sections 56.101 and 56.36, subdivision (b), of the Confidentiality of Medical Information Act (CMIA) (§ 56 et seq.) by negligently releasing class members' confidential medical information.

Several months after initiating the action, Vigil filed a motion for class certification. The trial court denied the motion, finding as to the CMIA claim

[1] Unless otherwise indicated, all statutory references are to the Civil Code.

that each class member would have to show that the confidential nature of his or her medical information had been breached by an unauthorized party, as required by *Sutter Health v. Superior Court* (2014) 227 Cal.App.4th 1546 (*Sutter Health*), and therefore that common issues would not predominate.

Vigil appeals, asserting that the trial court relied on an erroneous reading of the CMIA and that a breach of confidentiality can be shown on a class wide basis. We reject those arguments, and we affirm, concluding that the trial court properly applied the CMIA and exercised its discretion in denying class certification.

BACKGROUND

I.

The Data Breach and Vigil's Complaint

Muir is an independent practice association that consists of primary care and specialty care providers that provide medical services to patients through the John Muir Health system.

In May 2018, Ute Burness, Chief Executive Officer of Muir, notified certain patients that their personal information may have been involved in a data breach that occurred in December 2017. According to Burness, Muir discovered in March 2018 that a former employee took with her certain information in the possession of Muir before her employment ended with Muir (the data breach). The letter stated that Muir conducted an investigation, and "there is no evidence to date that your personal information has been misused in any way."[2] Vigil was one of the patients

[2] The trial court granted Muir's motion to file under seal some portions of the class certification papers and the supporting evidence. Accordingly, we will not divulge the content of the sealed portions of the record (Cal. Rules of Court, rule 8.46(b)(1)), which largely concern Muir's internal investigation of

who received this notice. Muir later admitted that the former employee, Myrissa Centeno, had downloaded copies of information for over 5,400 patients that included insurance and clinical information.

In July 2018, Vigil filed a class action complaint asserting causes of action for violation of the Customer Records Act (CRA) (§ 1798.80 et seq.), violation of the CMIA (§ 56 et seq.), unlawful and unfair business practices under the Unfair Competition Law (UCL) (Bus. & Prof. Code, § 17200 et seq.), and negligence. The UCL claim was predicated on the statutory and negligence claims. The complaint alleged that under the Health Insurance Portability and Accountability Act's (HIPAA) Security Management Process standard (45 C.F.R. § 164.308), Muir's employees should not have had access to records concerning approximately 5,500 patients without a "compelling" reason, nor should they have been able to take sensitive patient information with them. The complaint sought compensatory and punitive damages for Muir's alleged negligence in failing to secure plaintiffs' personal information. The complaint also alleged that this negligence violated the CRA.

The complaint further alleged that Muir violated sections 56.101, subdivision (a), and 56.36, subdivision (b), of the CMIA by negligently releasing patients' medical information without those patients' authorization. Accordingly, the complaint sought statutory damages under the CMIA for each class member.

II.

Motion for Class Certification

In September 2019, Vigil moved for class certification, appointment of her counsel as class counsel and appointment of herself as class

---

the data breach and the issue of whether Muir failed to take adequate measures to secure patients' confidential information.

representative. As pertinent here, Vigil contended that the complaint presented questions common to the class regarding whether Muir was negligent in handling class members' private medical information by failing to comply with its own HIPAA security policies, whether this negligence caused the data breach, and whether Centeno accessed and retained the private medical information without authorization. Vigil supported her motion with her declaration, citations to the depositions of two of Muir's HIPAA security officers and some of the deposition exhibits, including Muir's HIPAA policies, and Muir's discovery responses.

In opposition, Muir argued, among other things, that a CMIA claim requires a showing that the confidential nature of the plaintiff's medical information was breached, and that *Sutter Health*, *supra*, 227 Cal.App.4th 1546 held that there is no breach of confidentiality under the CMIA unless an unauthorized party has "actually viewed" the information. (*Id*. at p. 1550.) Thus, according to Muir, individualized issues of fact and law would predominate over the common questions because each putative class member would have to show that an unauthorized person viewed his or her confidential medical information.

In her reply, Vigil asserted that the case could be decided on a class-wide basis because there was evidence that Centeno downloaded, retained, and viewed a patient spreadsheet, and the CMIA does not require a showing that an unauthorized person read each line of medical data. In support, Vigil presented excerpts of the deposition of Janet Kesterson, Centeno's colleague at her current employer, that Vigil contended shows Centeno disclosed to Kesterson patient information she obtained from Muir. Kesterson testified that in March 2018, their employer tasked her and Centeno with traveling to offices to get phone numbers for Medicare members. Centeno told Kesterson

there was no need to go to those offices because she had the phone numbers, and she "lifted her phone and just scrolled real fast." Kesterson testified that she could not "decipher what information [Centeno] was scrolling through." She "could just tell it was an Excel spreadsheet."

Following a hearing on the motion, the trial court issued an order denying class certification. The court found that Vigil had conceded that the CRA does not apply to Muir, and thus the "crux" of Vigil's case "rest[ed] on her claim for breach of the Confidentiality of Medical Information Act."[3] It further found that the predominance of common questions requirement was not met because under the CMIA, "individualized inquiries would be required to prove Defendant's liability and damages to each of the nearly 5,500 proposed class members." Specifically, it concluded that "[l]iability for each class member is predicated on whether his or her information was ***actually viewed***, which on these facts is not capable of resolution in the aggregate."

Vigil appeals from the order denying class certification.

DISCUSSION

Vigil argues we should reverse the trial court's order because it relied on an erroneous reading of the CMIA in finding a predominance of individual issues. We conclude the trial court did not err in its application of the CMIA, and the class complaint's allegations raise questions regarding breach of confidentiality and causation that necessarily require individualized inquiries regarding many, if not all, of the putative class members. Those individualized issues predominate over common questions of law and fact, and thus we uphold the order denying class certification. (See *Linder v.*

---

[3] On appeal, Vigil does not dispute this finding, and thus for purposes of this appeal, we presume the trial court was correct in finding that the CRA does not apply here and that this matter turns on the CMIA claim. (See *Hewlett-Packard Co. v. Oracle Corp.* (2021) 65 Cal.App.5th 506, 563.)

Thrifty Oil Co. (2000) 23 Cal.4th 429, 436 (*Linder*) [" 'Any valid pertinent reason stated will be sufficient to uphold the order' "].)

I.

Legal Standards

A. The Governing Statutes

The CMIA protects the confidentiality of patients' medical information. (*Loder v. City of Glendale* (1997) 14 Cal.4th 846, 859.) It does so by prohibiting health care providers from disclosing a patient's medical information without authorization (§ 56.10) and imposing a duty on health care providers who create, maintain, or dispose of medical information to do so in a manner that preserves the confidentiality of that information (§ 56.101, subd. (a)). Subdivision (b) of section 56.36 provides remedies to patients for a health care provider's "release" of confidential medical information in violation of the CMIA. (§ 56.36, subd. (b).)

Here, Vigil alleges Muir violated section 56.101, subdivision (a), thereby invoking the remedy in section 56.36, subdivision (b). Subdivision (a) of section 56.101 provides in full, "Every provider of health care, health care service plan, pharmaceutical company, or contractor who creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information shall do so in a manner that preserves the confidentiality of the information contained therein. Any provider of health care, health care service plan, pharmaceutical company, or contractor 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." (§ 56.101, subd. (a).)

Section 56.36, subdivision (b), provides, in turn, "In addition to any other remedies available at law, any individual may bring an action against

any person or entity who has negligently released confidential information or records concerning him or her in violation of this part, for either or both of the following: [¶] (1) Except as provided in subdivision (e), nominal damages of one thousand dollars ($1,000). In order to recover under this paragraph, it is not necessary that the plaintiff suffered or was threatened with actual damages. [¶] (2) The amount of actual damages, if any, sustained by the patient."

B. The Case Law Interpreting Sections 56.36 and 56.101 of the CMIA

Sutter Health, *supra*, 227 Cal.App.4th 1546 and its predecessor, *Regents of University of California v. Superior Court* (2013) 220 Cal.App.4th 549 (*Regents*), are central to the parties' arguments in this appeal. Those cases address some of the requirements of a CMIA claim under sections 56.101, subdivision (a), and 56.36, subdivision (b), and hold that one such requirement is a breach of the confidentiality of the plaintiff's medical information.

In *Regents*, a thief stole an external hard drive and a card containing the hard drive's encryption password from the home of a physician working within the Regents health care system. (*Regents, supra*, 220 Cal.App.4th at p. 554.) The plaintiff, whose medical information was on the hard drive along with the medical information of more than 16,000 other patients, filed a complaint asserting a violation of the CMIA and seeking nominal damages for herself and for each of the more than 16,000 patients. (*Regents,* at pp. 554–555.) The complaint alleged that Regents failed to exercise due care to prevent the release or disclosure of the medical information, " 'and as a result it negligently lost possession of the hard drive and encryption passwords.' " (*Id.* at p. 555.) Regents demurred to the complaint, and the trial court overruled the demurrer. (*Id.* at pp. 555–556.) Regents sought a

writ of mandate requiring the trial court to sustain the demurrer, and the appellate court granted review of the trial court's ruling. (*Id.* at pp. 557, 571.)

On review, the court first noted that the parties did not dispute that the plaintiff had adequately alleged a violation of the duty imposed on Regents by section 56.101, subdivision (a), "to maintain and store medical information in a manner that preserves the confidentiality of that information." (*Regents*, *supra*, 220 Cal.App.4th at p. 560.) The court thus framed the issue before it as "the nature of [the remedy in section 56.36, subdivision (b)] as applied to the negligent maintenance or storage of medical information." (*Ibid.*) That section and the elements of the cause of action it creates, the court held, are incorporated by reference into section 56.101 and require a "release" of confidential information. (*Regents,* at pp. 561–562, 564.) Regents argued that the term "release" in section 56.36 was synonymous with "disclose" in section 56.10, subdivision (a), which requires a showing of an "affirmative communicative act" by the healthcare provider. (*Regents,* at p. 564.) The court disagreed, finding that under the common or ordinary dictionary meanings of those terms, "disclose" is an active verb, while "release" is broader and can include passive conduct. (*Ibid.*) It concluded, "a health care provider who has negligently maintained confidential medical information and thereby allowed it to be accessed by an unauthorized third person—that is, permitted it to escape or spread from its normal place of storage—may have negligently released the information within the meaning of CMIA." (*Id.* at p. 565.)

The *Regents* court went on to hold, however, that even under this broad interpretation of "release," pleading loss of possession was insufficient to state a cause of action under sections 56.101, subdivision (a), and 56.36, subdivision (b), for negligent maintenance or storage of confidential medical

information. (*Regents*, *supra*, 220 Cal.App.4th at pp. 569–570.) "What is required is pleading, and ultimately proving, 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.) The court noted in a footnote that section 56.101 allows a health care provider to dispose of, and therefore lose possession of, confidential medical records so long as the confidentiality of the records is preserved. (*Regents*, at p. 570, fn. 14.) In the case before it, no one knew what happened to the hard drive other than the thief that stole it, and thus the court concluded the plaintiff could not allege that her medical records "were, in fact, viewed by an unauthorized individual." (*Id.* at p. 570.) All she alleged was that Regents negligently lost possession of the medical information. (*Ibid.*) Accordingly, the court issued a writ of mandate directing the trial court to vacate its order overruling Regents' demurrer and to enter a new order sustaining the demurrer without leave to amend. (*Id.* at p. 571.)

The Third District decided *Sutter Health* the following year. *Sutter Health* involved a stolen desktop computer. (*Sutter Health*, *supra*, 227 Cal.App.4th at p. 1552.) Stored on the computer's hard drive were the medical records of more than four million patients in password-protected but unencrypted format. (*Ibid.*) The plaintiffs filed a complaint asserting violations of the CMIA. (*Sutter Health,* at p. 1552.) The defendant health care provider demurred, arguing the complaint did not state a claim under the CMIA because it did not allege that any unauthorized person had viewed the stolen medical information. (*Sutter Health,* at p. 1552.) The trial court overruled the demurrer, concluding the complaint sufficiently alleged a cause of action for breach of the CMIA. (*Sutter Health,* at p. 1552.) On a petition for writ of mandate challenging the order overruling the defendant's demurrer, the Court of Appeal agreed with *Regents* that the plaintiffs must

plead and prove a breach of confidentiality, and it clarified that "[n]o breach of confidentiality takes place until an unauthorized person views the medical information." (*Sutter Health,* at pp. 1553, 1555, 1557.)

The Third District arrived at this conclusion differently from the Second District, however. (*Sutter Health*, *supra*, 227 Cal.App.4th at p. 1555.) Unlike the *Regents* court, the *Sutter Health* court found that the duty of confidentiality imposed on health care providers by section 56.101 was not violated without an actual confidentiality breach, and that there was no need to consider the remedy provided in section 56.36 until such a violation occurred. (*Sutter Health,* at p. 1555.) The Third District relied on the first sentence of subdivision (a) of section 56.101—" 'Every provider of health care . . . who creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information shall do so in a manner that *preserves the confidentiality* of the information contained therein.' " (*Sutter Health,* at p. 1556.) This language, the court opined, "makes it clear that *preserving the confidentiality* of the medical information, not necessarily preventing others from gaining possession of the paper-based or electronic information itself, is the focus of the legislation. Therefore, if the confidentiality is not breached, the statute is not violated." (*Ibid.*) The first sentence of that subdivision "allows for change of possession as long as confidentiality is preserved." (*Ibid.*) The court further reasoned that "[n]o breach of confidentiality takes place until an unauthorized person views the medical information," because "[i]t is the medical information, not the physical record (whether in electronic, paper, or other form), that is the focus of the Confidentiality Act." (*Id.* at p. 1557.)

The court noted that the second sentence of section 56.101, subdivision (a), does not repeat the language in the first sentence imposing a

duty of confidentiality on the health care provider but this did not change its analysis because the second sentence makes the health care provider liable for negligence. (*Sutter Health*, *supra*, 227 Cal.App.4th at pp. 1557–1558.) Applying general negligence principles, the court found that "[t]he duty is to preserve confidentiality, and a breach of confidentiality is the injury protected against." (*Id.* at p. 1558.) "Without an actual confidentiality breach there is no injury and therefore no negligence under section 56.101." (*Ibid.*)

The court concluded the defendant did not violate section 56.101 because the plaintiffs had not alleged that their information was viewed. (*Sutter Health*, *supra*, 227 Cal.App.4th at p. 1559.) Accordingly, the court found that there was no reason to look to section 56.36 since it provides remedies only when a health care provider " 'has *negligently released* confidential information or records concerning [the plaintiff] *in violation of this part . . . .*' " (*Sutter Health*, at p. 1558.)

Although *Regents* and *Sutter Health* were decided at the pleading stage, both hold that a breach of confidentiality under sections 56.101, subdivision (a) and 56.36, subdivision (b) requires more than a showing that the health care provider negligently maintained or stored confidential information and lost possession of the information because of its negligence.

The interpretation of the CMIA in this case arises not on writ review of a demurrer ruling but on appeal from a ruling denying class certification. We turn, therefore, to the standards for class certification.

C. Class Certification Standards and Standards of Review

To properly allege a class, Vigil must "demonstrate the existence of an ascertainable and sufficiently numerous class, a well-defined community of

interest, and substantial benefits from certification that render proceeding as a class superior to the alternatives." (*Brinker Restaurant Corp. v. Superior Court* (2012) 53 Cal.4th 1004, 1021 (*Brinker*).) Community of interest, or commonality, encompasses three factors, including " 'predominant common questions of law or fact.' " (*Linder, supra*, 23 Cal.4th at p. 435.) "To establish the requisite community of interest, the proponent of certification must show, inter alia, that questions of law or fact common to the class predominate over the questions affecting the individual members . . . ." (*Washington Mutual Bank, FA v. Superior Court* (2001) 24 Cal.4th 906, 913.)

The denial of class certification to an entire class is an appealable order. (*Linder, supra*, 23 Cal.4th at p. 435.) We review a ruling on class certification for abuse of discretion. (*Brinker*, *supra*, 53 Cal.4th at pp. 1017, 1022.) A trial court ruling supported by substantial evidence will not be disturbed unless it rests on improper criteria or erroneous legal assumptions. (*Sav-On Drug Stores, Inc. v. Superior Court* (2004) 34 Cal.4th 319, 326–327.) We review de novo issues of statutory construction. (*Regents*, *supra*, 220 Cal.App.4th at p. 558.)

II.

Analysis

A. The Trial Court Did Not Err in Its Interpretation of the CMIA.

This class action is predicated on Muir's alleged negligence in maintaining and releasing confidential information in violation of sections 56.101, subdivision (a), and 56.36, subdivision (b), and thus Vigil and the putative class members must plead and prove that "the confidential nature of the plaintiff's medical information was breached as a result of the health care provider's negligence." (*Regents, supra*, 220 Cal.App.4th at p. 570.) Vigil appears to agree that Muir has not violated sections 56.101,

subdivision (a), and 56.36, subdivision (b), unless there is a breach of confidentiality. The parties dispute, however, what this showing entails and whether it is an individualized showing.

1. The Court Correctly Determined That a Breach of Confidentiality Requires an Unauthorized Person to Have "Actually Viewed" the Confidential Medical Information.

Vigil first argues that under *Regents*, confidential information that is "viewed, published, accessed, downloaded, copied, or otherwise *'permitted[] to escape from its normal place of storage*' " is "released" within the meaning of section 56.36, subdivision (b), and that a plaintiff need only show that the health care provider negligently "released" the confidential medical information to establish a claim under sections 56.36, subdivision (b), and 56.101, subdivision (a). She asserts that *Sutter Health* wrongly narrowed the *Regents* standard for a negligent release claim by requiring a showing that an unauthorized party "actually viewed" the confidential medical information to prove a breach of confidentiality.

Based on the statute's plain language, we agree with *Sutter Health* that a breach of confidentiality under the CMIA requires a showing that an unauthorized party viewed the confidential information. The CMIA does not define the term "confidential," but the ordinary meaning of the word supports *Sutter Health*'s "viewed" requirement. (*Angelucci v. Century Supper Club* (2007) 41 Cal.4th 160, 168 ["In interpreting a statute, we first consider its words, giving them their ordinary meaning and construing them in a manner consistent with their context and the apparent purpose of the legislation"].) The common or ordinary dictionary definition of "confidential" is "private" or "secret." (See, e.g., Black's Law Dict. (11th ed. 2019) p. 373, col. 1 ["meant to be kept secret]; Webster's Third New International Dict. (1961) p. 158, col. 1 ["private, secret"].) Thus, under the ordinary meaning of "confidential," the

confidential nature of information is not breached unless the information is reviewed by unauthorized parties. This construction is consistent with the purpose of the CMIA to protect patients' privacy. (See *Brown v. Mortensen* (2011) 51 Cal.4th 1052, 1071 ["[T]he interest protected by [the CMIA] is an interest in informational privacy"].)

Moreover, we also agree 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.) A breach of confidentiality thus entails more than mere loss of possession and does not "take[] place until an unauthorized person views the medical information." (*Id.* at p. 1557.)[4]

Vigil presents no basis for departing from *Sutter Health*. We disagree that *Sutter Health* "narrow[ed]" *Regents* by requiring more than mere loss of possession of medical records to establish a breach of confidentiality. After noting that the plaintiff could not "allege her medical records were, in fact, viewed by an unauthorized individual," the Second District held her pleading was "deficient" because it amounted to no "more than an allegation of loss of possession by the health care provider." (*Regents*, *supra*, 220 Cal.App.4th at p. 570.)

---

[4] Indeed, as the court in *Regents* stated, loss of possession is not necessarily required. "[A] breach of confidentiality, of course, can occur whether or not the information remains in the actual possession of the health care provider." (*Regents*, *supra*, 220 Cal.App.4th at p. 570, fn. 14.) It is an unauthorized person's *viewing* and/or *use* of another's medical records that violates the latter's interest in privacy of the information they contain.

Vigil relies on *Regents*' plain meaning construction of the term "release"—"permit[ting] [the confidential information] to escape or spread from its normal place of storage" and "allow[ing] it to be accessed" by an unauthorized party—as support for her argument. However, *Regents* does not stand for the proposition that mere loss of possession is sufficient on its own to prove a breach of confidentiality under sections 56.101, subdivision (a), and 56.36, subdivision (b). The *Regents* court opined that providing an unauthorized party access to confidential information "may" support a negligent release claim under the CMIA. (*Regents*, *supra*, 220 Cal.App.4th at p. 565.) But *Regents* expressly held that mere loss of possession was insufficient to establish a "release," even under a "broad interpretation" of that term. (*Id.* at p. 570.) By "release" in section 56.36, subdivision (b) "as incorporated into section 56.101," the Legislature intended "more than an allegation of loss of possession by the health care provider is necessary to state a cause of action for negligent maintenance or storage of confidential medical information." (*Regents*, at p. 570.)

Vigil points to other sections of the CMIA that use the term "release" as support for her argument that the Legislature intended section 56.36, subdivision (b), to refer to the actions of the custodian in "surrendering" or "mak[ing] available" private medical information to third parties. But those sections set forth the circumstances in which a health care provider may release medical information to the patient or to third parties; they do not impose liability on the health care provider for its "negligence." (Compare § 56.101, subd. (a) with §§ 56.11, 56.104, 56.07.) Muir, on the other hand, contends that the Legislature's use of the word "negligently" in sections 56.101 and 56.36 supports the conclusion in *Regents* and *Sutter*

Health that a breach of confidentiality under the CMIA requires more than a release of confidential information. We agree.

" 'The fundamental purpose of statutory construction is to ascertain the intent of the lawmakers so as to effectuate the purpose of the law.' " (*Realmuto v. Gagnard* (2003) 110 Cal.App.4th 193, 199.) As *Sutter Health* appears to have recognized in its application of general negligence principles (*Sutter Health*, *supra*, 227 Cal.App.4th at pp. 1557–1558), when the Legislature couches its enactment in common law language, we presume that it intended to carry over such rules as were part of the common law into statutory form. (*Presbyterian Camp & Conference Centers, Inc. v. Superior Court* (2021) 12 Cal.5th 493, 503 (*Presbyterian Camp*).) The essential elements of common law negligence are "the existence of a duty to use due care toward an interest of another that enjoys legal protection against unintentional invasion" (*Bily v. Arthur Young & Co.* (1992) 3 Cal.4th 370, 397), breach of that duty, injury, and causation (*Dixon v. City of Livermore* (2005) 127 Cal.App.4th 32, 42).

Vigil's interpretation of sections 56.36 and 56.101 conflicts with the presumption that the Legislature intended to incorporate those common law negligence principles. Imposing liability on a health care provider for the release of confidential information without a showing that an unauthorized party viewed the information would eliminate the injury and causation elements of negligence. "[T]he interest protected by [the CMIA] is an interest in informational privacy." (*Brown v. Mortensen*, *supra*, 51 Cal.4th at p. 1071; see also *Sutter Health*, *supra*, 227 Cal.App.4th at p. 1558 ["a breach of confidentiality is the injury protected against" by the CMIA].) Although sections 56.101 and 56.36 do not expressly state that a health care provider is liable only if its negligence caused a breach of confidentiality, it would be

inappropriate to read the causation and injury elements out of those sections, absent a clear expression by the Legislature of the intent to abrogate this common law. (See *Presbyterian Camp*, *supra*, 12 Cal.5th at p. 503.) No such intent appears here.

Vigil contends Sutter's reliance on the "duty of confidential[ity] that pervades CMIA" is misplaced because some courts have recognized that a breach of confidentiality can occur when the information is merely "disclosed" or "disseminated," regardless of whether unauthorized parties viewed the information. But the cases Vigil cites as support for this argument do not address the CMIA and are inapposite. None stand for the proposition that confidentiality is automatically breached whenever the confidential information is disseminated to unauthorized parties.

In *U.S. Dept. of Justice v. Landano* (1993) 508 U.S. 165, cited by Vigil, the court addressed the meaning of "confidential source" as used in an exemption from disclosure under the federal Freedom of Information Act (FOIA) for records compiled by criminal law enforcement authorities in the course of a criminal investigation. (*Landano,* at p. 167.) The exemption applies if the release of criminal investigation records " 'could reasonably be expected to disclose' the identity of, or information provided by, a 'confidential source.' " (*Ibid*.) In rejecting the defendant's argument "that a source is 'confidential' for purposes of [the exemption] only if the source can be assured, explicitly or implicitly, that the source's cooperation with the Bureau will be disclosed to no one," the court concluded "this cannot have been Congress' intent." (*Id.* at p. 171.) To read "confidential source" as meaning one given "[a] promise of complete secrecy" would mean "the FBI agent receiving the source's information could not share it even with other FBI personnel" and the information "would be of little use to the Bureau."

(*Id.* at p. 173.) The court's practical construction of the phrase "confidential source" in the context of the exemption from FOIA sheds no light on the nature of the CMIA's breach of confidentiality element.

Similarly inapposite is *Berkeley Police Assn. v. City of Berkeley* (2008) 167 Cal.App.4th 385 (*Berkeley Police Assn.*), in which the court held that interpreting a local ordinance to permit public hearings on citizen complaints against a police officer would conflict with provisions of the Police Officers Bill of Rights (POBRA) because it would result in disclosure of police personnel records those provisions required to be kept confidential. (*Berkeley Police Assn.,* at pp. 404–405.) The court's discussion of which records were confidential within the meaning of POBRA, which focused on earlier California Supreme Court authority interpreting the scope of POBRA's confidentiality provision and on the specific text of the relevant POBRA provisions (*Berkeley Police Assn.*, at pp. 395–402), likewise has no bearing on the meaning of the CMIA's language regarding health care providers' liability for breach of confidentiality.

The third case cited by Vigil, *Culinary Foods, Inc. v. Raychem Corp.* (N.D.Ill. 1993) 151 F.R.D. 297, addressed the request of plaintiff, Culinary, for a protective order for certain materials it sought to discover from Raychem and Raychem's request for a more restrictive order. The parties disputed whether Culinary could disseminate materials determined to be confidential to litigants and attorneys involved in similar actions against Raychem. (*Id.* at p. 306.) The court declined to allow such dissemination because it "would unduly raise the risk that Raychem's competitors will obtain access to this confidential information" and "make enforcement of this protective order overly burdensome to Raychem," as "evidenced by the fact that third parties have in fact received information in violation of protective

orders issued by other courts." (*Id.* at p. 307.) Insofar as Vigil's point in citing *Culinary Foods* is that allowing unauthorized access to confidential information can increase the risk that someone will view and/or make use that information, that is no doubt true. However, it does not answer the question of whether the Legislature, in adopting sections 56.36 and 56.101, intended to impose liability in situations where no actual invasion of the plaintiff's privacy occurs. Moreover, the *Sutter Health* court recognized that the change of possession of confidential information increases the risk of a confidentiality breach, but nonetheless held that the CMIA "does not provide for liability for increasing the risk of a confidentiality breach." (*Sutter Health*, *supra*, 227 Cal.App.4th at p. 1557.)

Vigil also asserts that a plaintiff would only have to show that an unauthorized party "downloaded" or "copied" confidential medical information to establish a claim under sections 56.36, subdivision (b), and 56.101, subdivision (a). However, she fails to present any cogent argument or legal authority in support of this conclusion in her opening brief.[5] In any

---

[5] In her reply, Vigil cites for the first time a federal case in support of her argument that a breach of confidentiality occurred when Centeno downloaded the patient spreadsheet and saved it to her personal phone or email account. Even assuming Vigil has not forfeited this argument (see *Paulus v. Bob Lynch Ford, Inc.* (2006) 139 Cal.App.4th 659, 685), that case is distinguishable because the plaintiff's claims arose from defendants' breach of *contractual,* not statutory, duties. (*Allergan, Inc. v. Merz Pharmaceuticals, LLC* (C.D.Cal., March 9, 2012, No. SACV 11-446 AG (Ex)) 2012 WL 781705, at p. *11.)

In her reply, Vigil also attempts to factually distinguish this case from *Sutter Health* based on evidence indicating that Centeno was aware of the contents of the patient spreadsheet and of its value to her new employer, that she downloaded it and retained it after her termination from Muir, and that she offered to provide the spreadsheet to her new employer. She fails to explain, however, why those facts show *Sutter Health* was wrongly decided.

event, a party that downloads or copies electronic files, as Centeno allegedly did in this case, does not necessarily breach confidentiality if the party has not actually viewed the confidential information included in the file. "It is the medical information, not the physical record (whether in electronic, paper, or other form), that is the focus of the Confidentiality Act)." (*Sutter Health*, *supra*, 227 Cal.App.4th at p. 1557.)

Finally, Vigil argues that the rule of *Sutter Health* will lead to unintended or absurd results. But interpreting sections 56.101 and 56.36 to impose liability on health care providers for the "release" of confidential information would expose health care providers to liability whenever an unauthorized party gains possession of the information, regardless of whether confidentiality was breached. On this issue, the *Sutter Health* court presented the example of a thief grabbing a computer containing medical information on four million patients and then wiping the hard drive without viewing the information. (*Sutter Health*, *supra*, 227 Cal.App.4th at p. 1558.) In that situation, the health care provider would be liable for at least $4 billion if we were to interpret section 56.101 as providing nominal damages to every person whose medical information came into the possession of an unauthorized person. (*Ibid.*) We do not believe the Legislature intended such an extreme result. By contrast, the CMIA's purpose of protecting the confidentiality of private medical information is preserved by interpreting those sections as requiring a showing that the confidentiality of the information was breached because of the health care provider's negligence.

Vigil cites *Stasi v. Inmediata Health Grp. Corp.* (S.D.Cal. 2020) 501 F.Supp.3d 898 (*Stasi*) as support for her argument. There, the defendant posted confidential medical information on the internet, "making it searchable, findable, viewable, printable, copiable, and downloadable by

anyone in the world with an internet connection." (*Id.* at p. 924.) Vigil argues that under "any conceivable standard," the confidentiality of the information at issue in that case was destroyed once it was published online, while that would not be the case under *Sutter Health* if the plaintiffs could not prove that an unauthorized party viewed their information. What she ignores is that the court in *Stasi* upheld *Sutter Health*'s "viewed" requirement. (*Stasi*, at p. 923.) There, on appeal from a motion to dismiss for failure to state a claim, the court found that the complaint's allegations gave rise to a reasonable inference that "someone" viewed the confidential information since it was accessible "by anyone in the world with an internet connection." (*Id.* at p. 924.) Thus, *Stasi* does not support Vigil's argument.

We therefore conclude the trial court correctly determined that a breach of confidentiality under sections 56.36, subdivision (b), and 56.101, subdivision (a), requires a showing that an unauthorized party viewed the confidential information at issue.

2. Vigil Has Not Shown That a Breach of Confidentiality Can Be Established on a Class-Wide Basis.

Vigil next challenges the trial court's finding that each class member would have to prove that his or her medical information was viewed by an unauthorized party. She argues that such a requirement cannot be found in section 56.36, *Sutter Health* or *Regents*. Instead, she claims, *Regents* shows that Vigil would not have to prove that Centeno read any of the information contained within the patient spreadsheet; her ability to access the information is sufficient under the CMIA. But, as previously discussed, the mere ability of an unauthorized party to access information cannot support a claim under sections 56.101, subdivision (a), and 56.36, subdivision (b). Vigil further contends that under *Sutter Health*, she need only show that Centeno

viewed the confidential records and not individual data entries. Muir disagrees, arguing that whether a breach of confidentiality under the CMIA occurred is an inherently individualized inquiry.

We agree that a breach of confidentiality under the CMIA is an individualized issue. *Regents* recognized that sections 56.36, subdivision (b), and 56.101, subdivision (a), provide a private cause of action for individual patients. This private cause of action, like the right of privacy, " ' "is purely a personal one." ' " (*Regents*, *supra*, 220 Cal.App.4th at p. 563 & fn. 6.) "The remedy provided in subdivision (b) [of section 56.36] is the right of an individual whose confidential information has been released in violation of CMIA to bring a private cause of action for nominal and/or actual damages." (*Id.* at p. 561.) For a negligent maintenance claim under section 56.101, subdivision(a), there is no "release[] . . . in violation of [the CMIA]" if there is no breach of confidentiality. (§§ 56.36, subd. (b), 56.101, subd. (a).) Accordingly, the individual bringing a private cause of action under those sections must establish that the confidential nature of his or her information was breached because of the health care provider's negligence. (See *Regents,* at p. 570.)

Contrary to Vigil's assertion in her opening brief, *Sutter Health* does not stand for the proposition that under the CMIA, a plaintiff need only show that an unauthorized party viewed some of the confidential information included in a medical record, regardless of whether the information viewed concerned the plaintiff. *Sutter Health* did not address this precise issue, which Vigil concedes in her reply.

Vigil contends that because a negligent release claim leads to lesser penalties under subdivision (b) of section 56.36 than an intentional release

claim under subdivision (c) of that section,[6] a negligent release claim requires a correspondingly less stringent evidentiary standard. But the legislative history she cites as support for this argument suggests that the purpose of the penalties under that section is deterrence, which in turn indicates that the increased penalties were intended to correspond with the increased culpability of the person or entity that discloses or uses medical information in violation of the CMIA. (See Assem. Com. on Judiciary, Analysis of Sen. Bill No. 19 (1999-2000 Reg. Sess.) July 13, 1999, p. 9 ["While the new civil penalties in the bill appropriately apply to 'knowing and willful' violations, the author believes that lesser penalties for negligent conduct that leads to an unauthorized disclosure should also be included in order to deter those releases as well"].) There is nothing in this history that suggests a negligent release claim does not require an individualized showing for the breach of confidentiality element.

Vigil argues for the first time in her reply that based on the plain language of section 56.36, subdivision (b), each class member would only have to prove that the medical *records* negligently released by the health care provider concerned them. Even assuming she has not forfeited this argument (*Paulus v. Bob Lynch Ford, Inc.*, *supra*, 139 Cal.App.4th at p. 685), it lacks merit. Section 56.36, subdivision (b), provides that the medical records or information must have been "negligently released . . . in violation of this part." (§ 56.36, subd. (b).) As mentioned, there is no "release[] . . . in

---

[6] Subdivision (c) of section 56.36 sets forth administrative fines and penalties to be imposed on a person or entity that uses or discloses medical information in violation of the CMIA. The amount of the fines and penalties increase when the use or disclosure is knowing and willful instead of negligent. (§ 56.36, subd. (c).)

violation of" section 56.101, subdivision (a), if the confidential nature of the information was not breached. (§§ 56.36, subd. (b), 56.101, subd. (a).)

Accordingly, we conclude that each class member would have to show that his or her medical information was viewed by an unauthorized party to recover under the CMIA.

B. The Trial Court Did Not Abuse Its Discretion in Finding a Predominance of Individual Issues.

Since Vigil has not shown that a breach of confidentiality can be established on a class wide basis, the question then is whether the common questions predominate over those individualized questions.

The key inquiry in determining whether the predominance requirement has been met is whether "the issues which may be jointly tried, when compared with those requiring separate adjudication, must be sufficiently numerous and substantial to make the class action advantageous to the judicial process and to the litigants." (*City of San Jose v. Superior Court* (1974) 12 Cal.3d 447, 460.) "Presented with a class certification motion, a trial court must examine the plaintiff's theory of recovery, assess the nature of the legal and factual disputes likely to be presented, and decide whether individual or common issues predominate." (*Brinker, supra,* 53 Cal.4th at p. 1025; see also *Ayala v. Antelope Valley Newspapers, Inc.* (2014) 59 Cal.4th 522, 530 [the question at the class certification stage is "whether the operative legal principles, as applied to the facts of the case, render the claims susceptible to resolution on a common basis"].)

" 'As a general rule if the defendant's liability can be determined by facts common to all members of the class, a class will be certified even if the members must individually prove their damages.' " (*Brinker*, *supra*, 53 Cal.4th at p. 1022.) However, "class treatment is not appropriate 'if every

member of the alleged class would be required to litigate numerous and substantial questions determining his individual right to recover following the "class judgment" ' on common issues." (*Duran v. U.S. Bank National Assn.* (2014) 59 Cal.4th 1, 28.) " 'Only in an extraordinary situation would a class action be justified where, subsequent to the class judgment, the members would be required to individually prove not only damages but also liability.' " (*Id.* at p. 30.) Here, based in part on *Sutter Health*'s "viewed" requirement, the trial court found that class treatment was not warranted because individualized inquiries would be required to prove Muir's liability and damages for each of the nearly 5,500 putative class members.

In challenging the trial court's determination, Vigil contends there are common questions regarding whether Centeno had unauthorized access to the patient spreadsheet and whether Muir was negligent in protecting that document. The evidence she presented on those issues below consists of the depositions of two of Muir's HIPAA security officers, a report from the investigation of the data breach, and Muir's policies. Based on this evidence, the question whether Muir failed to use due care in maintaining patients' private medical information is a significant issue susceptible to common proof. However, Vigil's burden "is not merely to show that some common issues exist, but rather, to place substantial evidence in the record that common issues *predominate*." (*Lockheed Martin Corp. v. Superior Court* (2003) 29 Cal.4th 1096, 1108.)

On this record, the trial court did not abuse its discretion in concluding individual issues would predominate over common issues. The record demonstrates that Centeno may have viewed some of the information on the patient spreadsheet, but Vigil presented no evidence indicating whose information was viewed. There is also no evidence suggesting that other

unauthorized parties viewed the information in the patient spreadsheet or that it was posted or disclosed in a public forum like the information at issue in *Stasi* or in *Berkeley Police Assn.* Therefore, most, if not all, of the almost 5,500 potential class members would be unable to maintain their CMIA claims against Muir unless they could establish that an unauthorized party viewed their confidential medical information and that Muir's negligence caused this breach of confidentiality.

In our research, we have not found any state cases, and the parties have not provided any, that concern the predominance requirement in a CMIA case or in a similar data breach action. The few federal cases that address CMIA claims, however, suggest that individual questions regarding whether a breach of confidentiality occurred and whether the health care provider's negligence caused the breach can be numerous and varied. In *In re Premera*, for example, the defendant was a health care provider that maintained patients' confidential information in a centralized database. (*In re Premera Blue Cross Customer Data Security Breach Litigation* (D.Or. 2016) 198 F.Supp.3d 1183, 1188.) In January 2015, it discovered that hackers had breached its computer network beginning in May 2014. (*Id.* at pp. 1189–1190.) The plaintiff subsequently filed a complaint for violation of the CMIA, which the defendant moved to dismiss. (*Premera,* at pp. 1190–1191.) The court concluded the plaintiff had adequately alleged a CMIA claim because in May 2015, she discovered on her credit report an inquiry for a car loan that she did not recognize, and her checking account had been fraudulently accessed "around the same time period." (*Premera,* at p. 1202.)

Similarly, in *Falkenberg*, the court determined on a motion to dismiss that plaintiffs had adequately alleged a claim for violation of the CMIA after a thief stole a password-protected laptop containing plaintiffs' and other

patients' confidential information. (*Falkenberg v. Alere Home Monitoring, Inc.* (N.D.Cal., Feb. 23, 2015, No. 13-cv-00341-JST) 2015 WL 800378, at pp. *1, *3.) The court found that the plaintiffs' CMIA claim was supported by allegations that their confidential medical information was viewed by an unauthorized party because they alleged that they gave the defendant that information, that they suffered identity theft sometime from three weeks to "weeks-and-months" from when the defendant's laptop containing the plaintiffs' information was stolen, that they had never suffered identity theft previously, that they took extra precautions to ensure their information was not disclosed to unknown third parties, and that the thieves opened fraudulent accounts using the plaintiffs' social security numbers, information that the defendant had and which was "not generally as available as date of birth, full name, and address." (*Falkenberg,* at p. *3.) The court noted that where a plaintiff claims a data breach caused them to be the victim of identity theft, there must be a " 'nexus' " between the alleged identity theft and the data breach " 'beyond allegations of time and sequence,' " and that there was such a nexus in that case. (*Id.* at p. *4.)

Applying the principles of those cases, the case here would require an assessment of each putative class member's circumstances to determine whether his or her information was viewed by an unauthorized party and whether the data breach caused this breach of confidentiality. This assessment includes questions regarding whether third parties used plaintiffs' information, whether this use was without authorization, the timing of this misuse, whether plaintiffs took measures to protect against the misuse of their information, whether the information used was involved in the data breach, and whether third parties could have obtained this information through other means.

Federal courts have denied class certification in data breach cases based on similar inquiries. (See *Gardner v. Health Net, Inc.* (N.D.Cal., Sept. 13, 2010, No. cv-10-2140) 2010 WL 11579028, at pp. *4–*5 [class treatment not warranted in data breach case where individualized inquiries would be required to prove the defendant's liability for negligence and other claims based on the injury and causation elements: "the theft of a potential class member's identity could be the result of any number of causes"]; *McGlenn v. Driveline Retail Merchandising, Inc.* (C.D.Ill., Jan. 19, 2021, No. 18-cv-2097) 2021 WL 165121, at pp. *8–*9 [the plaintiff failed to establish a predominance of common questions in data breach case involving almost 16,000 potential class members where the evidence showed that some putative class members may have suffered identity theft while others did not, and there were individualized issues on causation, given that some members were involved in other data breaches].)

We conclude substantial evidence supports the trial court's determination. On the record before us, each class member's "right to recover depends on facts peculiar to his case." (*City of San Jose v. Superior Court*, *supra*, 12 Cal.3d at p. 459; *Duran v. U.S. Bank National Assn.*, *supra*, 59 Cal.4th at p. 30.) Although it is only a general rule that a class cannot be maintained where liability turns on the facts of individual cases, the problems of proof here appear sufficiently pervasive and substantial as to support the trial court's denial of class certification based on the predominance of those questions.

DISPOSITION

The order is affirmed. Muir shall recover its costs on appeal.

STEWART, J.

We concur.

RICHMAN, Acting P.J.

MILLER, J.

Vigil v. Muir Medical Group (A160897)

Filed 10/18/22 after nonpublished opinion filed 9/26/22

CERTIFIED FOR PUBLICATION

IN THE COURT OF APPEAL OF THE STATE OF CALIFORNIA

FIRST APPELLATE DISTRICT

DIVISION TWO

MARIA VIGIL, Plaintiff and Appellant, v. MUIR MEDICAL GROUP IPA, INC., Defendant and Respondent.	A160897 (Contra Costa County Super. Ct. No. C1801331)

BY THE COURT:

The opinion in the above-entitled matter filed on September 26, 2022, was not certified for publication in the Official Reports. For good cause, the requests for publication are granted and pursuant to California Rules of Court, rule 8.1105, it now appears that the opinion should be published in the Official Reports, and it is so ordered.

Dated: _____

_____
RICHMAN, Acting P.J.

Trial Court: Contra Costa County Superior Court

Trial Judge: Hon. Edward G. Weil

Counsel:

Sommers Schwartz, Trenton R. Kashima; Finkelstein & Krinsk, Jeffrey R. Krinsk, John J. Nelson for Plaintiff and Appellant.

Reed Smith, Steven J. Boranian, David J. de Jesus, Emily F. Lynch for Defendant and Respondent.

Vigil v. Muir Medical Group IPA (A160897)