Filed 11/20/24 Doe v. Santa Cruz-Monterey-Merced Managed Medical Care Com. CA6

NOT TO BE PUBLISHED IN OFFICIAL REPORTS

IN THE COURT OF APPEAL OF THE STATE OF CALIFORNIA

SIXTH APPELLATE DISTRICT

JANE DOE, Plaintiff and Appellant, v. SANTA CRUZ-MONTEREY-MERCED MANAGED MEDICAL CARE COMMISSION et al., Defendants and Respondents.	H051515 (Santa Cruz County Super. Ct. No. 20CV02149)

I. INTRODUCTION

Plaintiff Jane Doe appeals after summary judgment was granted in favor of defendants Santa Cruz-Monterey-Merced Managed Medical Care Commission, Linda Forbes, Brenda Hill, and Heather Perko on plaintiff's claim for violation of the Confidentiality of Medical Information Act (CMIA) (Civ. Code, § 56 et seq.).[1] Santa Cruz-Monterey-Merced Managed Medical Care Commission, which does business as Central California Alliance for Health (Alliance), arranges for the provision of health care services to individuals with insufficient income. Plaintiff was a beneficiary of Alliance. The individual defendants –Forbes, Hill, and Perko – were employed by Alliance.

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

The individual defendants, who had Alliance e-mail accounts, were the victims of an e-mail phishing scam, which caused Alliance to experience a "data security breach." In a putative class action complaint, plaintiff alleged that defendants violated the CMIA by negligently creating, maintaining, preserving, and/or storing her confidential medical information, resulting in the release of her information during the data security incident. Defendants moved for summary judgment on various grounds, including that plaintiff had no evidence that an unauthorized third party actually viewed her confidential medical information. In opposition, plaintiff contended, among other arguments, that there was a triable issue regarding whether her medical information had actually been viewed. She also requested a continuance of the summary judgment hearing to conduct further discovery. The trial court denied the continuance, granted the motion for summary judgment, and filed a judgment in favor of all defendants.

On appeal, plaintiff contends that the trial court erred in granting defendants' summary judgment motion and in denying her request for a continuance. For reasons that we will explain, we will affirm the judgment.

II. FACTUAL BACKGROUND

Defendant Alliance was formed by three counties in order to arrange for the provision of health care services to individuals with insufficient income. In this regard, Alliance operated a program that provided primary care through a contracted provider network for Medi-Cal recipients. During the relevant timeframe of late April 2020, to early May 2020, Alliance employed defendants Forbes, Hill, and Perko in administrative roles. Plaintiff has been a member or beneficiary of Alliance since 2015.

Between late April and early May 2020, Alliance experienced a "data security breach." Specifically, Alliance employees received e-mails from another organization whose e-mail accounts, unbeknownst to Alliance, had been compromised. A third party subsequently gained unauthorized access to certain Alliance employee e-mail accounts.

Alliance's IT department received a report of suspicious e-mails from defendant Forbes's account. The unauthorized third party had accessed Forbes's e-mail account and used her account to send out "phishing emails" to others. The unauthorized third party would have been able to access Forbes's entire e-mail history and any member information that was included in Forbes's e-mail account. Forbes's e-mail account contained a 2017 e-mail that had been sent to her and several other recipients. That 2017 e-mail contained an attachment with medical information about plaintiff and others. Some of the phishing e-mails sent from Forbes's account in 2020 went to some of the people who had also been recipients of the same 2017 e-mail as Forbes. The IT department investigated and took action regarding Forbes's account.

The next day, the IT department was notified about suspicious e-mails from defendant Hill's account. The IT department took action regarding Hill's account and continued to investigate the matter. It was discovered that the e-mail account of defendant Perko had also been compromised.

Alliance subsequently provided written notice to members whose confidential medical information was found within the three compromised Alliance e-mail accounts of Forbes, Hill, and Perko. None of the three compromised Alliance e-mail accounts would have included members' financial information or social security number.

Of the three compromised Alliance e-mail accounts, information about plaintiff was contained only in the attachment to the 2017 e-mail that was in defendant Forbes's e-mail account. Forbes was one of several recipients of the 2017 e-mail. There was no information about plaintiff in the body of the 2017 e-mail. Regarding the attachment to the 2017 e-mail, plaintiff's information was in a single row in the latter half of several thousand rows in a spreadsheet. The information regarding plaintiff did not include financial information, social security number, address, e-mail address, or telephone number.

Although plaintiff in a special interrogatory response stated that an unauthorized party actually viewed her electronic medical information, she did not disclose any fact that

would directly support this statement. For example, she did not identify evidence that the 2017 e-mail, or the spreadsheet attached to the e-mail, was opened by an unauthorized third party. Plaintiff herself does not know whether the 2017 e-mail or the attached spreadsheet was opened as a result of the data security incident. Plaintiff's discovery responses indicated that she had no evidence of her medical information being misused or disclosed by an unauthorized third party as a result of the security incident.

III. PROCEDURAL BACKGROUND

A. *The Civil Action*

In the operative third amended putative class action complaint, which was filed in February 2022, plaintiff alleged a single cause of action against defendants Alliance, Forbes, Hill, and Perko for violating the CMIA. Plaintiff alleged that defendants negligently created, maintained, preserved, and/or stored her confidential medical information, resulting in the release of her information in violation of section 56.101, subdivision (a) of the CMIA.[2] According to plaintiff, an unauthorized third party accessed and actually viewed her medical information. She sought nominal and actual damages under the CMIA. (§ 56.36, subdivision (b)(1), (2).) Alliance and the individual defendants filed answers to the operative pleading.

B. *Defendants' Motion for Summary Judgment*

On May 12, 2023, defendant Alliance and the individual defendants filed a motion for summary judgment. Defendants contended (1) that plaintiff had no evidence that an unauthorized third party actually viewed her confidential medical information, which is required to prevail on a claim under section 56.101, subdivision (a) of the CMIA, and no evidence of any other substantive violation of the CMIA, and (2) that any defendant was among the entities or persons who may be held liable under the CMIA. The hearing on the motion was set for August 4, 2023.

[2] Plaintiff also alleged that defendants violated section 56.10, subdivision (a). She does not pursue this theory of liability on appeal.

C. *Plaintiff's Ex Parte Application to Continue Summary Judgment Hearing*

On July 17, 2023, approximately two months after defendants filed their summary judgment motion and a few days before plaintiff's opposition was due on July 21, 2023, plaintiff filed an ex parte application to continue the summary judgment hearing pursuant to Code of Civil Procedure section 437c, subdivision (h). In a supporting declaration, plaintiff's counsel contended that a continuance was necessary (1) to complete the depositions of five people who were scheduled to be deposed on July 13, 14, 18, and 21, 2023; (2) to obtain the transcripts for those depositions; and (3) to allow plaintiff's expert to review the transcripts. Plaintiff's counsel argued that the July deposition dates were the result of accommodating the witnesses' availability pursuant to communications with defense counsel. Plaintiff's counsel also contended that although two of the five depositions had already been taken, those depositions provided information that supported plaintiff's expert's opinion that plaintiff's medical information was actually viewed by an unauthorized person. Further, according to counsel, information from one of the depositions indicated that the "native file" of a PDF document needed to be produced and a further deposition was needed regarding that document.

Defendants filed opposition to the continuance request. They contended that plaintiff did not attempt to take the depositions until almost three years after the case had been filed, which reflected a lack of diligence, and that plaintiff otherwise failed to provide a good faith justification for the continuance.

On July 18, 2023, the trial court denied without prejudice plaintiff's ex parte application for a continuance.

D. *Plaintiff's Opposition to Defendants' Summary Judgment Motion*

On July 21, 2013, plaintiff filed an opposition to defendants' motion for summary judgment, and she again requested a continuance of the hearing pursuant to Code of Civil Procedure section 437c, subdivision (h).

Regarding a continuance, plaintiff contended that additional time was needed to allow her "to file the relevant portions of the certified copies of the deposition transcripts of [five Alliance] employee witnesses (Luis Somoza, Bob Trinh, Paul Mealiffe, Manuel Coto, and Magdalena Kowalska) taken within the last 7 Court days . . . ; and/or in order to obtain an electronic copy of Exhibit 3 to the . . . Somoza declaration filed in support of the [summary judgment motion], and to take the further deposition of . . . Somoza; and/or to submit a supplemental declaration [from plaintiff's expert] Matt Strebe . . . ." In a supporting declaration, plaintiff's counsel indicated that he had taken Somoza's deposition on July 13, Trinh's deposition on July 14, and Mealiffe's deposition on July 18 and that he would complete the depositions of Coto and Kowalska on July 21. Counsel stated that Somoza's and Trinh's depositions "will support Plaintiff's allegations in her operative complaint that [her] medical information was accessed and actually viewed by the unauthorized third party 'attacker[.]' " Plaintiff's counsel stated that defense counsel had designated Somoza's and Trinh's transcripts as confidential, but that he (plaintiff's counsel) could "generally" state that both deponents "testified that an unauthorized person accessed the email account containing Plaintiff's medical information and testified to facts concerning the Data Breach that support's Plaintiff's expert opinion that Plaintiff's medical information was actually viewed by an unauthorized person."

Regarding the substance of the summary judgment motion, plaintiff contended that there was a triable issue as to whether her medical information had actually been viewed. She also argued that she could establish the other elements required for a violation of section 56.101, subdivision (a) of the CMIA, including that defendant Alliance was a health care service plan and defendant Forbes was a provider of health care.

Plaintiff also filed a July 21, 2023 declaration from her expert, Matthew Strebe, who was the founder of an information technology business, had conducted security audits and forensic data breach investigations, and had been an expert witness and consultant in data breach cases. Strebe had reviewed the discovery in the case, including the "rough," but not

yet certified, deposition transcripts of employees of defendant Alliance. Strebe believed that Alliance's security before the data breach was inadequate and that its investigation after the breach was insufficient.

Strebe explained that the attacker could have downloaded all of the e-mail in a user's mailbox. Strebe opined that it was "more likely than not that the . . . attacker also used [this function] to access and exfiltrate the entire contents of [defendants Forbes's, Hill's, and Perko's] . . . mailboxes during the [p]hishing [a]ttack and was a proximate cause of the release of [p]laintiff's" information.

According to Strebe, "human attackers read through the email contents, viewing any interesting data they may find, especially large files, image files, and other content which has a high likelihood of relevance to their monetization schemes." Strebe stated, "There is no reason for attackers to exfiltrate or steal emails (and their attachments) that they do not view. Stealing information and not using that information would serve no purpose."

Strebe also opined, based on his experience and based on the discovery in the case, that it was "more likely than not" that an "unauthorized person searched the entire contents of [defendant Forbes's] . . . mailbox and actually viewed the results during the [p]hishing [a]ttack," and that it was "more likely than not" the unauthorized person "actually viewed [plaintiff's medical information] set forth in the . . . attachment . . . to the 2017 [e]mail . . . contained in [Forbes's] . . . mailbox during the [p]hishing [a]ttack."

One of plaintiff's counsel submitted a declaration regarding his "dark web searches" for plaintiff's "[p]ersonal [i]dentity [i]nformation," including her "name and address." Plaintiff's name along with her address and/or phone number were apparently found on a website for a company that operated a mobile banking application in mid-2020.

In her own declaration, plaintiff stated that she never submitted her name, address, or other personal identity information to the banking service company. She further stated that she received a notice of a class action settlement involving that banking service company in or about July 2023. The notice pertained to a data breach between June 23 and July 1, 2020,

that apparently occurred at the banking service company. According to the notice, the settlement class members were "all California residents, as confirmed by having a California address on file in [the banking service company's] business records at the time of the [d]ata [b]reach, whose [p]ersonal [i]dentity [i]nformation . . . was subjected to the [d]ata [b]reach, as confirmed by [the banking service company's] business records."

E. *Defendants' Reply*

Defendants contended that plaintiff had not made a good faith showing that a continuance of the summary judgment hearing was warranted. On the merits of the summary judgment motion, defendants argued that plaintiff's evidence was insufficient to create a triable issue regarding whether her medical information was actually viewed. Defendants contended that Strebe's opinion – that it was more likely than not that the attacker viewed plaintiff's information – was speculation and conjecture. Defendants argued that a third party's access to the medical information is insufficient to show actual viewing and that plaintiff's opposition did not contain any facts demonstrating actual viewing. Further, defendants contended that plaintiff could not establish that either Alliance or Forbes was subject to liability under the CMIA. Defendants observed that plaintiff had not disputed that defendants Hill and Perko were not subject to liability under the CMIA.

F. *The Hearing on Defendants' Summary Judgment Motion*

The hearing on defendants' summary judgment motion was held on August 4, 2023. Prior to the hearing, the trial court issued a tentative ruling (1) denying plaintiff's request to continue the hearing and (2) granting defendants' motion for summary judgment. At the hearing, plaintiff contended that there was sufficient evidence to infer that her medical information had actually been viewed. Defendants contended that the evidence was insufficient and that it was instead "complete speculation."

G. *The Trial Court's Order*

On August 7, 2023, the trial court filed a written order. The court denied plaintiff's request to continue the hearing, finding among other things that plaintiff failed to show "facts that controverting evidence may exist" and failed to show good cause or diligence.

Regarding the summary judgment motion, the trial court granted defendants' requests for judicial notice, and granted in part and denied in part plaintiff's requests for judicial notice. The court declined to consider defendants' evidentiary objections because there was no proof of service on plaintiff. The court overruled all of plaintiff's evidentiary objections, which consisted of a paragraph of objections that were repeated verbatim in response to numerous facts in defendants' separate statement. The court explained regarding plaintiff's objections that it could not "discern, and decline[d] to parse through, each objection to determine its applicability."

In granting defendants' summary judgment motion, the trial court explained that to establish a negligent release of confidential medical information under section 56.36, subdivision (b), and section 56.101, subdivision (a), the information must actually be viewed by an unauthorized person. The court found that the opinion of plaintiff's expert Strebe – that plaintiff's information was actually viewed – was not supported by the evidence. The court determined that neither "[v]iewing the email in which [p]laintiff's information was attached," nor "using an email embedded in the stolen document to continue the attack" was sufficient. In "considering all inferences in favor of" plaintiff, the court found that "[n]o material factual dispute has been shown from which a jury could reasonably conclude that [p]laintiff's confidential medical information was actually viewed as a result of the 2020 phishing attack on [defendant] Alliance."

The trial court also determined that plaintiff could not establish a violation of any of the other provisions of the CMIA. The court further stated that plaintiff had no evidence that defendant Alliance was a health care service plan, contractor, provider of health care, or

authorized recipient under the CMIA, nor any evidence that Alliance or any individual defendant provided plaintiff with medical services.

On September 1, 2023, a judgment was entered in favor of all defendants. Plaintiff thereafter filed a notice of appeal.

IV. DISCUSSION

Plaintiff contends that the trial court erred in granting defendants' motion for summary judgment because there is a triable issue of material fact regarding whether her medical information was viewed. She also argues that there are triable issues regarding the other elements of a claim for a violation of the CMIA, including whether defendants Alliance and Forbes are health care providers. Further, plaintiff contends that the court abused its discretion in denying her request for a continuance of the summary judgment hearing.

We observe that defendants in their responding brief state that plaintiff "does not appear to contest the grant of summary judgment as to [d]efendants Brenda Hill or Heather Perko as [plaintiff's opening] brief includes no argument pertaining to their purported liability." Plaintiff does not contend otherwise in her reply brief on appeal. We will therefore affirm the judgment as to defendants Hill and Perko. Regarding the remaining defendants (Alliance and Forbes), as we shall explain, the trial court properly granted summary judgment on the ground that plaintiff failed to create a triable issue of material fact regarding whether her medical information was viewed, and the trial court did not abuse its discretion in refusing to continue the summary judgment hearing.

A. *Defendants' Motion for Summary Judgment*

1. Standard of Review

A party moving for summary judgment "bears an initial burden of production to make a prima facie showing of the nonexistence of any triable issue of material fact; if [the movant] carries [this] burden of production," the burden of production shifts to the opposing party "to make a prima facie showing of the existence of a triable issue of material fact."

(*Aguilar v. Atlantic Richfield Co.* (2001) 25 Cal.4th 826, 850 (*Aguilar*).) A defendant moving for summary judgment may meet the initial burden of production by "present[ing] evidence that conclusively negates an element of the plaintiff's cause of action" or by "present[ing] evidence that the plaintiff does not possess, and cannot reasonably obtain, needed evidence—as through admissions by the plaintiff following extensive discovery to the effect that he [or she] has discovered nothing." (*Id.* at p. 855, fn. omitted.)

In determining whether the parties have met their respective burdens, "the court must 'consider all of the evidence' and 'all' of the 'inferences' reasonably drawn therefrom [citation], and must view such evidence [citations] and such inferences [citations], in the light most favorable to the opposing party." (*Aguilar, supra,* 25 Cal.4th at p. 843; see Code Civ. Proc., § 437c, subd. (c) ["the court shall consider . . . all inferences reasonably deducible from the evidence"].) "There is a triable issue of material fact if, and only if, the evidence would allow a reasonable trier of fact to find the underlying fact in favor of the party opposing the motion in accordance with the applicable standard of proof." (*Aguilar, supra,* at p. 850, fn. omitted.)

"In reviewing a trial court's grant of summary judgment, . . . ' "[w]e take the facts from the record that was before the trial court when it ruled on that motion" ' and ' " ' "review the trial court's decision de novo . . . ." ' " ' " (*Hughes v. Pair* (2009) 46 Cal.4th 1035, 1039.)

2. Plaintiff's Evidentiary Objections

Plaintiff's separate statement contained evidentiary objections to facts from defendants' separate statement.[3] The trial court observed that plaintiff's evidentiary objections were contained in a paragraph that was "repeated verbatim" to every disputed

[3] We note that the California Rules of Court require written "[o]bjections to specific evidence" to "be served and filed separately from the other papers" in opposition to a motion for summary judgment and "not be restated or reargued in the separate statement." (Cal. Rules of Court, rule 3.1354(b); see *Universal City Studios Credit Union v. CUMIS Ins. Society, Inc.* (2012) 208 Cal.App.4th 730, 734, fn. 1.)

fact of defendants. The court stated that plaintiff's "verbatim objections are overruled," explaining that it could not "discern, and declines to parse through, each objection to determine its applicability."

On appeal, plaintiff contends that "the trial court failed to specifically rule on [her] objections" and "[t]hus, [her] evidentiary objections are properly reviewed de novo." The record reflects, however, that the court expressly overruled all of plaintiff's objections.

Moreover, plaintiff fails to demonstrate that the trial court erred in overruling her objections. Plaintiff does not dispute that she repeatedly asserted the same set of boilerplate objections to each disputed fact from defendants' separate statement. Her evidentiary objections were not directed to specific *evidence*, but were instead directed to defendants' *facts* contained in their separate statement – facts that were based on multiple pieces of evidence. As a result, the trial court was unable to "discern, and decline[d] to parse through, each objection to determine its applicability." We, likewise, are unable to discern and decline to parse through each objection to determine its applicability to unspecified pieces of evidence. Plaintiff fails to demonstrate error by the trial court in overruling her evidentiary objections under these circumstances. (See *Hodjat v. State Farm Mutual Automobile Ins. Co*. (2012) 211 Cal.App.4th 1, 7-9 [holding that evidentiary objections should have been directed to pieces of evidence, not facts in the opposing party's separate statement, and that the trial court did not error in refusing to rule on the objections].)

3. Confidentiality of Medical Information Act

a. *Background*

The CMIA generally requires a health care provider to maintain medical information in a manner that preserves its confidentiality, and a negligent failure to do so may result in legal liability. (§§ 56.101, subd. (a), 56.36, subd. (b).) The CMIA " 'is intended to protect the confidentiality of individually identifiable medical information obtained from a patient by a health care provider [and related entities], while at the same time setting forth limited circumstances in which the release of such information to specified entities or individuals is

permissible.' [Citations.]" (*Brown v. Mortensen* (2011) 51 Cal.4th 1052, 1070; see also *Regents of University of California v. Superior Court* (2013) 220 Cal.App.4th 549, 553 (*Regents*).)

b. *Relevant provisions*

At the time of the incident in this case, the CMIA defined medical information as "any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care, health care service plan, pharmaceutical company, or contractor regarding a patient's medical history, mental or physical condition, or treatment. 'Individually identifiable' means that the medical information includes or contains any element of personal identifying information sufficient to allow identification of the individual, such as the patient's name, address, electronic mail address, telephone number, or social security number, or other information that, alone or in combination with other publicly available information, reveals the individual's identity." (§ 56.05, former subd. (j), amended by Stats. 2013, ch. 444, § 2.)[4]

Regarding liability, section 56.101, subdivision (a) states: "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 subdivision[] (b) . . . of Section 56.36."

Section 56.36, subdivision (b), in turn, authorizes a civil action "against a person or entity who has negligently released confidential information or records concerning" the plaintiff in violation of the CMIA. The remedies include statutory damages and actual

[4] The CMIA's definition of medical information has since been amended in ways not relevant here.

damages. (§ 56.36, subd. (b)(1) [authorizing "nominal damages of one thousand dollars"], (2) [authorizing actual damages].)

c. *Establishing liability*

A "breach of the confidentiality of the plaintiff's medical information" must be shown in order to establish a claim under sections 56.101, subdivision (a), and 56.36, subdivision (b). (*Vigil v. Muir Medical Group IPA, Inc*. (2022) 84 Cal.App.5th 197, 209 (*Vigil*); see *Sutter Health v. Superior Court* (2014) 227 Cal.App.4th 1546, 1556, 1557 (*Sutter*) [explaining that § 56.101, subd. (a) focuses on "preserving the confidentiality of the medical information" (italics omitted) and that liability arises under this subdivision "for failing to 'preserve[] the confidentiality' of the medical records"]; *Regents*, *supra*, 220 Cal.App.4th at p. 570 [holding that to establish a defendant "negligently released confidential information or records" under § 56.36, subd, (b), as incorporated into § 56.101, a plaintiff must prove "that the confidential nature of the plaintiff's medical information was breached as a result of the health care provider's negligence" (fn. omitted)].) Otherwise, "[i]mposing 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." (*Vigil*, *supra*, at p. 215.)

To show a breach of confidentiality under section 56.101, subdivision (a), and section 56.36, subdivision (b), there must be proof that the medical information "was improperly viewed or otherwise accessed." (*Regents*, *supra*, 220 Cal.App.4th at p. 554; accord, *Vigil*, *supra*, 84 Cal.App.5th at p. 213 ["the confidential nature of information is not breached unless the information is reviewed by unauthorized parties"].) Mere "loss of possession" of the medical information by the health care provider is insufficient to show a breach of confidentiality. (*Regents*, *supra*, at p. 570.) Likewise, it has been held that "[t]he mere possession of the medical information or records by an unauthorized person [is] insufficient to establish breach of confidentiality if the unauthorized person has not viewed the information or records." (*Sutter*, *supra*, 227 Cal.App.4th at p. 1553.) "No breach of

confidentiality takes place until an unauthorized person views the medical information. It is the medical information, not the physical record (whether in electronic, paper, or other form), that is the focus of the [CMIA]." (*Id.* at p. 1557.) Although a "change of possession" may "increase[] the risk of a confidentiality breach," "the [CMIA] does not provide for liability for increasing the risk of a confidentiality breach." (*Ibid.*) Similarly, "[w]hile loss of possession may result in breach of confidentiality, loss of possession does not necessarily result in a breach of confidentiality." (*Ibid.*)

For example, in *Regents*, *supra*, 220 Cal.App.4th 549, the plaintiff patient alleged that an encrypted external hard drive containing medical information of patients treated at the defendant's health facilities, along with an index card containing the password for the encrypted information, was stolen from the home of a physician who had brought the hard drive home. (*Id.* at p. 554.) The appellate court observed that, "[b]ecause no one (except perhaps the thief) knows what happened to the encrypted external hard drive and the password for the encrypted information, [the plaintiff] cannot allege her medical records were, in fact, viewed by an unauthorized individual." (*Id.* at p. 570.) In the absence of such an allegation, the appellate court concluded that the defendant's "demurrer should have been sustained without leave to amend and the case dismissed." (*Ibid.*)

A similar conclusion was reached in *Sutter*, *supra*, 227 Cal.App.4th 1546. In *Sutter*, a thief broke into an office and stole the defendant health care provider's desktop computer, which contained the medical records of more than four million patients. (*Id.* at p. 1552.) The medical records "were stored on the computer's hard drive in password-protected but unencrypted format." (*Ibid.*) The appellate court determined that the plaintiff patients had failed to state a cause of action because they did "not allege that the stolen medical information was actually viewed by an unauthorized person." (*Id.* at p. 1550.) The appellate court explained that to interpret the CMIA to provide $1,000 in statutory damages "to every person whose medical information came into the possession of an unauthorized person without that person viewing the information would lead to unintended results. For

example, if 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. For all we know, that may have happened here. We cannot interpret a statute to require such an unintended result. [Citations.]" (*Sutter, supra,* at p. 1558.)

Similarly, in *Vigil, supra,* 84 Cal.App.5th 197, a former employee of the defendant medical group downloaded information for over 5,400 patients. (*Id.* at p. 206.) The information was contained in a spreadsheet, and there was evidence that the former employee had " 'scrolled real fast' " through " 'an Excel spreadsheet.' " (*Id.* at p. 207.) However, there was "no evidence indicating whose information was viewed." (*Id.* at p. 221.) The appellate court affirmed denial of class certification, concluding that the plaintiff patient failed to show that a breach of confidentiality could be established on a classwide basis. (*Id.* at pp. 218–219; see *id.* at p. 207.) The appellate court explained that "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)." (*Id.* at pp. 218–219.) Further, it was not sufficient for the plaintiff to "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." (*Id.* at p. 219.) Instead, "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," which meant that "each class member would have to show that his or her medical information was viewed by an unauthorized party." (*Id.* at pp. 219, 220.) In the absence of evidence that an unauthorized party viewed the information or that it was posted in a public forum, the appellate court observed that "most, if not all, of the almost 5,500 potential class members would be unable to maintain their CMIA claims against [the defendant] unless they could establish that an unauthorized party viewed their confidential

medical information and that [the defendant's] negligence caused this breach of confidentiality." (*Id.* at p. 221.)

In contrast, in *J.M. v. Illuminate Education, Inc*. (2024) 103 Cal.App.5th 1125, review granted Oct. 30, 2024, S286699, the defendant, an education consulting business, obtained the plaintiff's personal and medical information from the plaintiff's school and its office of education to assist the school. (*Id.* at p. 1129.) A "cyber hacker gained access" to the plaintiff's personal information in the defendant's possession. (*Ibid.*) Thereafter, third parties mailed solicitations to plaintiff at an address that he had only provided to the defendant through the office of education. (*Ibid.*) The appellate court determined that "[a]llegations that a plaintiff has received increased spam after the data breach" supported an inference that the plaintiff's medical information had been viewed by an unauthorized third party. (*Id.* at p. 1134; see also *ibid.* [sufficient allegations that personal information was actually viewed by others].)

4. Analysis

To show a breach of confidentiality under section 56.101, subdivision (a), and section 56.36, subdivision (b), there must be proof that the medical information "was improperly viewed or otherwise accessed." (*Regents, supra,* 220 Cal.App.4th at p. 554; accord, *Vigil, supra*, 84 Cal.App.5th at p. 213 ["the confidential nature of information is not breached unless the information is reviewed by unauthorized parties"].) In this case, defendants presented evidence that within the three compromised Alliance e-mail accounts, plaintiff's medical information was contained only in one attachment to a 2017 e-mail in defendant Forbes's account. Her information was not in the body of the e-mail but rather was in a single row among several thousand rows in the attachment. The information in the attachment did not include plaintiff's financial information, social security number, address, e-mail address, or telephone number. Although some of the people who previously received the 2017 e-mail also received "phishing emails" from Forbes's e-mail account, Alliance provided evidence that the 2017 e-mail was not the source for the additional phishing e-

mails. In a written discovery response, plaintiff stated that an unauthorized party had actually viewed her electronic medical information, but the facts that she disclosed did not sufficiently support this statement to create a triable issue of material fact. For example, she did not identify evidence that the 2017 e-mail, or the spreadsheet attached to the e-mail, was opened by an unauthorized third party. Plaintiff herself did not know whether the e-mail or the attached spreadsheet was opened. Plaintiff's discovery responses also indicated that she had no evidence of her medical information being misused or disclosed by an unauthorized third party as a result of the security incident.

In opposition to defendants' summary judgment motion, plaintiff failed to demonstrate a triable issue of material fact regarding whether there was a breach of confidentiality.

First, regarding case law holding that an unauthorized person must actually view the medical information, plaintiff seeks to distinguish *Sutter, supra*, 227 Cal.App.4th 1546, and *Regents, supra*, 220 Cal.App.4th 549, on the ground that those cases involved information that was encrypted or password protected, whereas her information was not. According to plaintiff, the data in those cases "remained secured in a proverbial lock box," and "there were no facts that the encryption or password had been defeated." We understand plaintiff to be contending that the appellate courts in those cases required the plaintiffs to show that the medical information had actually been viewed in order to establish a breach of confidentiality under the CMIA in view of the fact that the information was encrypted or password protected.

We are not persuaded that the actual viewing requirement only applies in cases where the medical information was encrypted or password protected. In *Regents*, although the information was encrypted, an index card containing the password for the encrypted information was apparently stolen at the same time as the hard drive. (*Regents*, *supra*, 220 Cal.App.4th at p. 554.) The appellate court concluded that the plaintiff "cannot allege her medical records were, in fact, viewed by an unauthorized individual," and the court

concluded that the defendant's "demurrer should have been sustained without leave to amend and the case dismissed." (*Id.* at p. 570.) Similarly, in *Vigil*, a former employee downloaded information for over 5,400 patients, and there is no indication in the case that the information was encrypted or password protected. (*Vigil*, *supra*, 84 Cal.App.5th at p. 206.) In fact, there was evidence that the former employee had " 'scrolled real fast' " through " 'an Excel spreadsheet.' " (*Id.* at p. 207.) Nonetheless, the appellate court observed that there was "no evidence indicating whose information was viewed." (*Id.* at p. 221.) The appellate court determined that it was not sufficient for the plaintiff to "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." (*Id.* at p. 219.) The appellate court concluded that "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)." (*Id.* at pp. 218–219.)

Second, plaintiff fails to provide evidence from which an inference may reasonably be drawn that her medical information contained in the 2017 e-mail attachment in Forbes's account was accessed let alone actually viewed. (See *Aguilar*, *supra*, 25 Cal.4th at p. 843 ["a court must 'consider all of the evidence' and 'all' of the 'inferences' reasonably drawn therefrom"]; Code Civ. Proc., § 437c, subd. (c) ["the court shall consider . . . all inferences reasonably deducible from the evidence"].) Indeed, the evidence in this case is less than in *Vigil*, where the appellate court found insufficient evidence of actual viewing based on a former employee who downloaded information for thousands of patients and " 'scrolled real fast' " through " 'an Excel spreadsheet.' " (*Vigil*, *supra*, 84 Cal.App.5th at pp. 206, 207.)

Plaintiff's evidence of actual viewing in this case includes the following:

The unauthorized party who engaged in the phishing attack in 2020 would have been able to access defendant Forbes's entire e-mail history and any member information that was included in Forbes's e-mail account. From this evidence, however, it is speculation whether the unauthorized party actually accessed the 2017 e-mail in Forbes's e-mail

account, opened the attachment to that e-mail, and viewed plaintiff's medical information, which was contained within in a single row in the latter half of several thousand rows in a spreadsheet.

Next, among the several people who originally received the 2017 e-mail, some of them also received phishing e-mails from Forbes's e-mail account. However, Alliance provided evidence that the 2017 e-mail was not the source for the additional phishing e-mails. Under these circumstances, it would be speculation to conclude that the 2017 e-mail was accessed or viewed, let alone to conclude that plaintiff's information in the attachment to the 2017 e-mail was accessed or viewed.

There also evidence that Alliance provided written notice to members, including plaintiff, whose confidential medical information was found within the three compromised Alliance e-mail accounts of Forbes, Hill, and Perko. The notice, however, indicates only that health information "may" have been accessed or disclosed. This notice does not establish that plaintiff's medical information was actually accessed or viewed.

The declaration from plaintiff's expert, Strebe, is also insufficient to create a triable issue regarding whether plaintiff's medical information in the attachment to the 2017 e-mail was viewed. Strebe indicated that a "monetization scheme" is the purpose of a phishing attack. In this case, however, there is no evidence that the 2017 e-mail or its attachment involved a monetary transaction such that a reasonable inference might arise that the 2017 e-mail was accessed and viewed by the attacker to further a "monetization scheme." To the contrary, the undisputed evidence reflected that none of the e-mail accounts for defendants Forbes, Hill, or Perko included members' financial information or social security number.

Although the 2017 e-mail contained an attachment with medical information, Strebe's declaration does not indicate whether the particular medical information contained in that attachment, including regarding plaintiff, had any relevance to a "monetization scheme." Moreover, there was no evidence that any medical information contained in the compromised Alliance e-mail accounts had been used in a monetization scheme. Further,

plaintiff's own attorney conducted dark web searches and did not report that he found any medical information regarding plaintiff. Under these circumstances, Strebe's general statements regarding phishing attacks are insufficient to create a triable issue regarding whether the 2017 e-mail was accessed and opened, its attachment was opened, and plaintiff's confidential information, among the thousands of rows of information, was viewed.

Strebe further opined that "[t]here is no reason for attackers to exfiltrate or steal emails (and their attachments) that they do not view. Stealing information and not using that information would serve no purpose." Here, however, there was no evidence that the attacker did "exfiltrate or steal" the 2017 e-mail or its attachment.

Strebe also opined that it was "more likely than not" that the attacker exfiltrated or stole the entire contents of the mailboxes belonging to defendants Forbes, Hill, and Perko. However, other than Strebe's opinion that the attacker would have had the ability to do so, there was no evidence that the attacker actually did so.

In view of these broad and general statements by Strebe about phishing attacks with little or no connection to or support from the specific facts in this case, we determine that his opinion that it was "more likely than not" the unauthorized person "actually viewed [plaintiff's medical information] set forth in the . . . attachment . . . to the 2017 [e]mail . . . contained in [Forbes's] . . . mailbox during the [p]hishing [a]ttack" to be speculation.

Third, plaintiff contends that dark web search results and her receipt of a class action settlement notice for a banking service company show that her "individually identifiable information" (§ 56.05, subd. (j)) was misused to open an unauthorized financial account at the company's website after the phishing attack on defendant Alliance. Plaintiff argues that the misuse of her information by the banking service company shows that her Alliance information was actually viewed.

The CMIA protects medical information, not individually identifiable information by itself. (§§ 56.101, subd. (a), 56.05, subd. (j).) In this case, the misused information on the

banking service company's website consisted of plaintiff's name along with her address and/or phone number. However, the 2017 Alliance e-mail attachment did not contain her address or phone number (nor did the attachment contain her social security number, e-mail address, or any financial information). Further, none of the compromised Alliance e-mail accounts belonging to defendants Forbes, Hill, and Perko would have included members' financial information or social security number. As a result, it would not be reasonable to infer from the existence of the financial account that the financial account had been opened using information from the attachment to the 2017 e-mail and that plaintiff's medical information in the attachment was actually viewed.

Fourth, plaintiff cites to several federal cases in support of her contention that there is evidence that her medical information was actually viewed. The federal cases cited by plaintiff, however, do not advance her argument. To the extent the cases involve a CMIA claim, those cases involved different facts and merely addressed the sufficiency of the pleading, not whether there was sufficient evidence to create a triable issue in opposition to a summary judgment motion. (See *Stasi v. Inmediata Health Group Corp*. (S.D.Cal. 2020) 501 F.Supp.3d 898, 923 [determining that the plaintiffs' complaint was sufficient where they "allege[d] their information 'was viewed by unauthorized persons' " (fn. omitted)]; *In re Solara Medical Supplies, LLC Customer Data Security Breach Litigation* (S.D.Cal. 2020) 613 F.Supp.3d 1284, 1299 [finding that the plaintiffs' complaint sufficiently alleged an unauthorized viewing where they pleaded "an increase in medical-related spam emails and phone calls following the data breach"]; *Corona v. Sony Pictures Entertainment, Inc*. (C.D.Cal., June 15, 2015, No. 14-CV-09600 RGK EX) 2015 WL 3916744, pp. *1, *8 [holding that the plaintiffs' allegations that personal information was stolen, used to threaten the victims and their families, and posted on the internet; that the defendant "fail[ed] to maintain the confidentiality of their medical information"; that their medical information was released; and that the defendant "admitted to the compromise of [the] protected health information" were sufficient].)

We therefore conclude that plaintiff failed to create a triable issue of material fact regarding whether her medical information was accessed, let alone viewed, such that there was a breach of confidentiality of plaintiff's medical information in violation of the CMIA by defendant Alliance or Forbes. In view of our conclusion, we need not reach the issues of whether defendant Alliance or Forbes falls within the statutorily defined categories of individuals or entities that are subject to liability under the CMIA, or whether plaintiff must prove that she received healthcare from a defendant.

B. ***Denial of Plaintiff's Request for a Continuance***

Plaintiff contends that the trial court abused its discretion in denying her request for a continuance of the summary judgment hearing. Plaintiff's first request for a continuance was made a few days before she filed her opposition to the summary judgment motion, and the trial court denied her request without prejudice. We understand plaintiff on appeal to be challenging the ruling regarding her second continuance request, which was included in her written opposition to defendants' summary judgment motion and which the trial court denied.

Code of Civil Procedure section 437c, subdivision (h) states: "If it appears from the affidavits submitted in opposition to a motion for summary judgment . . . that facts essential to justify opposition may exist but cannot, for reasons stated, be presented, the court shall deny the motion, order a continuance to permit affidavits to be obtained or discovery to be had, or make any other order as may be just." "We review a court's ruling on a request for a [Code of Civil Procedure] section 437c, subdivision (h) continuance for abuse of discretion. [Citation.] 'Notwithstanding the court's discretion in addressing such continuance requests, "the interests at stake are too high to sanction the denial of a continuance without good reason." [Citation.] Thus, "[t]o mitigate summary judgment's harshness, the statute's drafters included a provision making continuances—which are normally a matter within the broad discretion of trial courts—virtually mandated ' "upon a good faith showing by

affidavit that a continuance is needed to obtain facts essential to justify opposition to the motion." ' " ' [Citation.]

"To make the requisite good faith showing, an opposing party's declaration must show (1) the facts to be obtained are essential to opposing the motion, (2) there is reason to believe such facts may exist, and (3) the reasons why additional time is needed to obtain these facts. [Citation.] The reason for this 'exacting requirement' [citation] is to prevent 'every unprepared party who simply files a declaration stating that unspecified essential facts may exist' [citation] from using the statute 'as a device to get an automatic continuance' [citation]. 'The party seeking the continuance must justify the need, by detailing both the particular essential facts that may exist and the specific reasons why they cannot then be presented.' [Citation.]" (*Chavez v. 24 Hour Fitness USA, Inc*. (2015) 238 Cal.App.4th 632, 643 (*Chavez*).) " 'It is not sufficient under the statute merely to indicate further discovery or investigation is contemplated. The statute makes it a condition that the party moving for a continuance show "facts essential to justify opposition may exist." ' [Citation.]" (*Cooksey v. Alexakis* (2004) 123 Cal.App.4th 246, 254 (*Cooksey*).)

"Even absent a sufficient declaration, 'the court must determine whether the party requesting the continuance has nonetheless established good cause therefor.' " (*Chavez, supra*, 238 Cal.App.4th at p. 643, citing *Lerma v. County of Orange* (2004) 120 Cal.App.4th 709, 716.) Considerations for a continuance include "whether the evidence sought is truly essential to the motion." (*Chavez*, *supra*, at p. 644.)

Some courts have questioned whether, or to what extent, the plaintiff's diligence in completing discovery should be considered in deciding whether to grant a continuance. (See *Braganza v. Albertson's LLC* (2021) 67 Cal.App.5th 144, 154–155 [discussing cases].) Consistent with the majority of courts (*Cooksey*, *supra*, 123 Cal.App.4th at p. 257), this court has determined that diligence is a relevant factor (see, e.g., *Chavez*, *supra*, 238 Cal.App.4th at p. 644 ["the requesting party's lack of diligence is relevant to the inquiry"]; *Rodriguez v. Oto* (2013) 212 Cal.App.4th 1020, 1038).

In this case, plaintiff sought a continuance to (1) file "relevant portions" of the certified copies of the deposition transcripts of five Alliance employees – Somoza, Trinh, Mealiffe, Coto, and Kowalska, and/or (2) "to obtain an electronic copy" of exhibit 3 to Somoza's declaration and to take a further deposition of him, and/or (3) to submit a supplemental declaration from plaintiff's expert Strebe.

The trial court denied plaintiff's request, finding that the declaration from her counsel was insufficient. Among other things, the court found that counsel "does not show facts that controverting evidence may exist and why that information is essential . . . ." The court also observed that plaintiff did not "finally decide[]" to take depositions until nearly three years after the action was filed and more than 16 months after the filing of the operative third amended complaint. The court believed that plaintiff's inability "to provide the requisite affidavit for good cause [was] at least in part based on her own lack of diligence in pursuing oral discovery in this action . . . ." We determine that the court did not abuse its discretion in denying plaintiff's request for a continuance in view of her failure to " 'detail[] . . . the particular essential facts' " that would justify a continuance. (*Chavez, supra*, 238 Cal.App.4th at p. 643; see also *id.* at p. 644.)

First, plaintiff did not explain the relevance of either Coto's or Kowalska's deposition testimony, or otherwise " 'detail[] . . . the particular essential facts that may exist' " in either deposition. (*Chavez, supra*, 238 Cal.App.4th at p. 643; see *id.* at p. 644.)

Second, regarding Somoza's and Trinh's depositions, plaintiff's counsel failed in his declaration to " 'detail[] . . . the *particular* essential facts that may exist' " in Somoza's and Trinh's depositions that would have justified the need for a continuance. (*Chavez*, *supra*, 238 Cal.App.4th at p. 643, italics added.)

For example, plaintiff's counsel in his declaration stated that Somoza's and Trinh's depositions "will support Plaintiff's allegations in her operative complaint that [her] medical information was accessed and actually viewed by the unauthorized third party 'attacker[.]' " Plaintiff's counsel further stated that defense counsel had designated Somoza's and Trinh's

transcripts as confidential, but that he (plaintiff's counsel) could "generally" state that both deponents "testified that an unauthorized person accessed the email account containing Plaintiff's medical information and testified to facts concerning the Data Breach that support's Plaintiff's expert opinion that Plaintiff's medical information was actually viewed by an unauthorized person." These broad, general, nonspecific statements – that the depositions contain facts about the data breach that support plaintiff's expert's opinion that plaintiff's medical information was actually viewed – are insufficient. Plaintiff's counsel was required to " 'detail[] . . . the *particular* essential facts that may exist' " in Somoza's and Trinh's depositions that would justify the need for a continuance. (*Chavez*, *supra*, 238 Cal.App.4th at p. 643, italics added.) Plaintiff acknowledges that rough transcripts were available, and her expert Strebe acknowledges that he reviewed them, yet counsel's declaration lacked the requisite particularity needed to justify a continuance. Plaintiff cites *Dee v. Vintage Petroleum, Inc*. (2003) 106 Cal.App.4th 30, among other cases, contending they are "nearly identical" to her case. However, none of the cases stand for the proposition that a plaintiff is entitled to a continuance even if the declaration from counsel fails to detail the particular essential facts that the plaintiff claims may exist. For example, in *Dee*, the counsel's declaration included the specific testimony from the deposition that warranted a continuance. (*Dee*, *supra*, at p. 34.)

For the first time on appeal, plaintiff broadly contends that "[m]aterial deposition statements impeach[ed]" Somoza's and Trinh's declarations that were filed in support of defendants' summary judgment motion. In support of this contention, plaintiff cites numerous paragraphs in her counsel's declaration and in her expert's declaration (both filed in opposition to the summary judgment motion) that describe defendant Alliance's purported inadequate security before the phishing attack and insufficient investigation after the attack. Plaintiff does not adequately identify the deposition testimony that she contends were material and impeaching, nor does she otherwise sufficiently " 'detail[] . . . the

particular essential facts that may exist' " in the depositions to justify a continuance. (*Chavez*, *supra*, 238 Cal.App.4th at p. 643; see *id.* at p. 644.)

Third, regarding the purported need for discovery concerning exhibit 3 to Somoza's declaration, plaintiff failed to show that facts concerning the exhibit were " 'essential' " to opposing the summary judgment motion. (*Chavez*, *supra*, 238 Cal.App.4th at pp. 643, 644.) Exhibit 3 to Somoza's declaration contained excerpts from the 2017 e-mail attachment, including plaintiff's medical information. Somoza, who was an employee of Alliance and in charge of the phishing incident response, stated in his declaration that plaintiff's information was in a "hidden" tab in the attachment. According to plaintiff, however, Somoza indicated at his deposition that the PDF document contained in exhibit 3 did not actually show or support this statement that plaintiff's information was hidden from view "but that the native .xlsx document (which was never produce[d] before his deposition) does." Plaintiff sought a continuance in order to "obtain a copy of the .xlsx native file . . . and to re-depose Luis Somoza on Exhibit #3 attached to his declaration . . . ."

Whether plaintiff's information, or the tab, was hidden in the 2017 e-mail attachment was not a fact " ' essential' " to opposing defendants' summary judgment motion. (*Chavez*, *supra*, 238 Cal.App.4th at pp. 643, 644.) The trial court did not rely on this fact in granting summary judgment, nor have we in concluding that summary judgment was properly granted. Moreover, even assuming the fact of whether plaintiff's information or the tab was hidden, plaintiff's expert Strebe already disputed that fact in his declaration. On this record, obtaining a different copy of the file and/or further deposing Somoza would have either (1) further supported defendants' contention that the information or tab was hidden, or (2) been cumulative to plaintiff's expert's statement that the information or tab was not hidden. Under either scenario, further discovery on the issue was not essential to plaintiff's opposition to the summary judgment motion.[5]

[5] We also note that, contrary to plaintiff's assertion on appeal that the trial court determined that the native file was essential, the court's order reflects no such express

Fourth, given that plaintiff counsel's declaration was deficient concerning the need for further discovery, counsel's declaration was also deficient in showing a need for a continuance to obtain a supplemental declaration from plaintiff's expert Strebe regarding "such new evidence."

In sum, plaintiff failed to provide a sufficient declaration from counsel to justify a continuance. (See *Chavez*, *supra*, 238 Cal.App.4th at p. 643.) Even aside from the declaration, plaintiff failed to establish good cause for a continuance because she did not show that the proposed discovery was "truly essential" (*id.* at p. 644), including with respect to certified transcripts and regarding whether her medical information was hidden in the 2017 e-mail attachment. On this record, even without considering whether plaintiff had been diligent in discovery, we determine that the trial court did not abuse its discretion in denying plaintiff's request to continue the summary judgment hearing based on her failure to show the particular essential facts that may exist and which would justify a continuance. (See *id.* at pp. 643, 644.)

Accordingly, plaintiff fails to demonstrate that the trial court erred in granting defendants' motion for summary judgment.

V. DISPOSITION

The judgment is affirmed.

---

finding. Instead, the court simply referred to plaintiff's counsel's *assertion* that the file was important. Specifically, the court stated, "While Plaintiff argues that she is prejudiced by the deposition timeline in this case, her counsel does not include the information required for showing good cause for a continuance. He describes the deposition setting process and its delays, but he does not show facts that controverting evidence may exist and why that information is essential (except for the native file he asserts supports a portion of the Somoza Declaration), and he fails to describe the specific reasons why evidence could not be presented in the Opposition and the steps he will take to obtain the evidence."

BAMATTRE-MANOUKIAN, ACTING P. J.

WE CONCUR:

DANNER, J.

WILSON, J.

Doe v. Santa Cruz-Monterey-Merced Managed Medical Care Commission et al.
H051515