THE DOCTOR IS IN, BUT YOUR MEDICAL INFORMATION IS OUT

Trends in California Privacy Cases Relating to Release of Medical Information

By Joseph R. Tiffany II, Connie J. Wolfe, Ph.D. and Allen Briskin[1]

Privacy breaches continue to be big news. In California, breaches of health care information are particularly sensitive, due to a number of state laws that provide legal remedies not available in other jurisdictions. While California's Civil Code sections 1798.29, 1798.82 and its Unfair Competition Law ("UCL")[2] are often relied on to remedy breaches of privacy, California also has the Confidentiality of Medical Information Act ("CMIA"),[3] providing that an individual may recover $1,000 in nominal damages (plus actual damages if any) based on the negligent release of medical information by a health care provider or other covered party. As health care providers have moved toward the storage of medical data in large electronic databases containing information regarding many thousands of individuals, the potential number of people who may be affected by a single unauthorized release of medical information and the accompanying potential liability have skyrocketed. Until the past two years, however, there was little published authority interpreting the CMIA's definition of "medical information" or its prohibition on the "release" of such information. California courts have now provided guidance on these two critical issues affecting the potential liability of providers and others who sustain health care data breaches.

I. SCOPE OF THE CMIA

The CMIA, enacted in 1981 and since amended several times, obligates any "provider of health care, health care service plan, pharmaceutical company or contractor" to maintain "medical information . . . in a manner that preserves the confidentiality of the information contained therein."[4] "Contractors" under the CMIA include medical groups, independent practice associations, certain pharmaceutical benefits managers and medical service organizations. The CMIA has recently been broadened to cover businesses that are "organized for the purpose of maintaining medical information" and "any business that offers software or hardware to consumers, including a mobile application or other related device that is designed to maintain medical information" (e.g., personal health record vendors), even though such entities are excluded from the definition of "provider of health care for purposes of any law other than this part, [section 56.06]."[5]

---

1 Joseph R. Tiffany II is a partner in Pillsbury Winthrop Shaw Pittman LLP's Antitrust & Competition Practice Group. Connie J. Wolfe is a special counsel in Pillsbury Winthrop Shaw Pittman LLP's Antitrust & Competition Practice Group. Allen Briskin is a senior counsel in Pillsbury Winthrop Shaw Pittman LLP's Health Care & Life Sciences Practice Group. This article reflects the views of the authors and not necessarily those of Pillsbury Winthrop Shaw Pittman LLP, its attorneys, or its clients.

2 Cal. Bus. & Prof. § 17200 *et seq.*

3 Cal. Civ. Code § 56 *et seq.*

4 Cal. Civ. Code § 56.101.

5 *Id.* § 56.06(a), (b).

The CMIA generally prohibits the disclosure of an individual's medical information without the individual's authorization, unless a specific exception applies or the disclosure is required by law.[6] Health care providers and other parties subject to the CMIA are prohibited from sharing, selling, using for marketing purposes or otherwise using medical information for a purpose not necessary to provide health care services unless "expressly authorized."[7] In addition, the CMIA requires *employers* who obtain employee medical information to handle it confidentially and similarly prohibits their unauthorized disclosure of such information.[8]

The CMIA applies only to "medical information," which is defined 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."[9]

Under this definition, for information to constitute "medical information," three elements must be established:

(1) There must be individually identifiable information regarding an individual's medical history, mental or physical condition, or treatment;

(2) Such information must be in the possession of or derived from a provider of health care, health care service plan, pharmaceutical company, or contractor; and

(3) Such information must pertain to a "patient" of a provider of health care, i.e., one who has received health care services from that provider of health care.

The CMIA also includes a detailed list of specific medical information *excluded* from coverage under the Act. Data found in certain types of public social services records, industrial accident documentation,[10] and law enforcement records, among other sources, are on the exclusion list.[11]

Violations of the CMIA are subject to harsh penalties, which are in addition to any other remedies available to a plaintiff.[12] Such damages and penalties include:

Damages for Economic Loss: Any patient who has sustained economic loss or personal injury resulting from violation of any of the following prohibitions may recover

---

6 *Id.* § 56.10(a).

7 *Id.* § 56.10(d), (e).

8 *Id.* § 56.20.

9 *Id.* § 56.05(j).

10 The CMIA clarifies, however, that even to the extent certain industrial accident information may be disclosed under section 56.30(f), disclosure of a patient's HIV status is not permitted without prior authorization from the patient unless the patient claims that the infection or exposure to HIV arose in the course of his or her employment.

11 Cal. Civ. Code § 56.30.

12 *Id.* § 56.35.

compensatory damages; punitive damages (not to exceed $3,000); attorneys' fees (not to exceed $1,000); and the costs of litigation.[13] The prohibitions include: unauthorized "disclosure" of a patient's medical information; [14] unauthorized "release" of information regarding outpatient psychotherapy treatment;[15] violation of the CMIA's limitations on the use and disclosure of medical information by employers;[16] and third party administrators' "knowingly" using, disclosing or permitting its employees or agents to use or disclose medical information, except as reasonably necessary in connection with the administration or maintenance of the program, or with authorization.[17]

Damages for Negligent Disclosure: Any covered party "who negligently creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information"[18] in violation of California Civil Code section 56.101 is subject to the following remedies under section 56.36(b): nominal damages of $1,000 (which does not require "that the plaintiff suffered or was threatened with actual damages");[19] and/or actual damages, if any.

Civil/Criminal Penalties: If a violation of the CMIA results in an economic loss or personal injury to a patient, it is punishable as a misdemeanor.[20] For negligent disclosures, an administrative remedy or civil penalty of up to $2,500 per violation may be assessed.[21] A person or entity (other than a licensed health care professional) who knowingly and willfully "obtains, discloses, or uses medical information in violation of [the CMIA] shall be liable for an administrative fine or civil penalty not to exceed $25,000 per violation."[22] If the violation was carried out "for . . . purpose[s] of financial gain," the penalty may be increased to $250,000 per violation and violators are also subject to disgorgement of any proceeds of that unlawful use.[23] Licensed health care professionals are subject to staggered penalties, ranging from $2,500 to $25,000 per violation.[24] If such professionals engaged in the violation "for financial gain," the penalty ranges from $5,000 to $250,000 per violation (for the third and subsequent violations), and disgorgement is also *available at* the highest tier.[25]

---

13 *Id.*

14 *Id.* § 56.10.

15 *Id.* § 56.104.

16 *Id.* § 56.20.

17 *Id.* § 56.26(a).

18 *Id.* § 56.101.

19 *Id.* § 56.36(b)(1).

20 *Id.* § 56.36(a).

21 *Id.* § 56.36(c)(1).

22 *Id.* § 56.36(c)(2)(A).

23 *Id.* § 56.36(c)(3)(A).

24 *Id.* § 56.36(c)(2)(B).

25 *Id.* § 56.36(c)(3)(B).

II. JUDICIAL INTERPRETATION OF THE SCOPE OF MEDICAL INFORMATION UNDER THE CMIA

In the years since the CMIA was implemented, various California courts have provided some guidance in further defining the term "medical information." The California Supreme Court clarified that the accuracy of the information is not at issue–a CMIA claim does not require a plaintiff to show that the disclosure was false or misleading.[26] In addition, the California Court of Appeal for the Second District held that the term "medical information" under the CMIA is "broadly defined" and "[t]here is no question that 'the patient's name, address, age, and sex' when combined with 'a general description of the reason for treatment'; 'the general nature of the injury'; and 'the general condition of the patient' comprise 'medical information.'"[27] In another case, the Court of Appeal for the Second District held that the fact that a patient "received in vitro fertilization was clearly 'medical information' as defined in section 56.05, subdivision (g)."[28] In contrast, an anesthesiologist's loud verbal review of a patient's chart, including her HIV status, in a location where other patients could overhear was held not to violate the CMIA when there was no evidence that potential listeners were able to see the patient during the discussion and the defendant did not use the plaintiff's full name, or disclose any other individually identifying information specified in the statute that would disclose her identity.[29]

Consequently, since the CMIA's enactment, it has been unclear just how broadly the term "medical information" could be defined. As a result, until last year's decision in *Eisenhower Medical Center v. Superior Court (Malanche),* 226 Cal.App.4th 430 (Cal. Ct. App. 2014), it remained possible that the term could be construed as broadly as is the term "individually identifiable health information" under the Health Insurance Portability and Accountability Act ("HIPAA"), the federal statute providing privacy and security standards for health information. For example, in the preamble to the HIPAA Privacy Rule,[30] the Department of Health and Human Services ("HHS") stated that a record that simply identifies the individual and provides the name of a health care provider that has provided unspecified services to the patient (e.g., hospital or physician) can, without any additional information being present, constitute individually identifiable health information. The HHS's approach appears to be based on the reasoning that an individual's provider-patient relationship with a specific health care provider is information that "relates" broadly to the individual's health or condition, or health care

---

26 *Brown v. Mortensen*, 253 P.3d 522, 533-34 (Cal. 2011).

27 *Garrett v. Young*, 109 Cal. App. 4th 1393, 1406 (Cal. Ct. App. 2003) (citation omitted) (holding that physician's disclosure to the plaintiff's employer that she suffered from itching and stress fell within a statutory exemption to the prohibition against disclosure of medical information, and that plaintiff had waived any right of recovery under the CMIA by openly discussing her conditions with supervisor and co-workers).

28 *Colleen M. v. Fertility and Surgical Associates of Thousand Oaks*, 132 Cal. App. 4th 1466, 1475 (Cal. Ct. App. 2005).

29 *Maureen K. v. Tuschka, M.D.*, 215 Cal. App. 4th 519 (Cal. Ct. App. 2013) (upholding summary judgment on a plaintiff's CMIA claim based on loud discussions of her medical history in a pre-operative room).

30 45 C.F.R. §§ 160, 164(A), 164(E), 165.

received, and thus information may legally "relate" to an individual's health or condition without divulging anything substantive about it. In the same way, "medical information" under the CMIA, defined as information that "regards" a patient's medical history or physical condition, could potentially be deemed to apply to information as limited as the name of the health care provider who had a relationship with the individual.

In the *Eisenhower* case, a unanimous three-judge panel of the California Court of Appeal, Fourth Appellate District, examined whether a patient index containing personal identifying information qualifies as medical information under the CMIA, and held that it did not.[31]

The facts in *Eisenhower* involved the theft of a computer that contained an index of over 500,000 persons to whom the Eisenhower Medical Center ("EMC") had assigned a clerical record number and included each person's name, medical record number, age, birth date, and the last four digits of their social security number.[32] The medical record numbers were issued sequentially and did not contain any coded information. The computer was password-protected but not encrypted. EMC moved for summary judgment on the ground "that the index did not contain medical information within the meaning of the CMIA."[33] The trial court denied EMC's motion "based principally on its belief that the fact that a person was a patient at the hospital is medical information within the meaning of the CMIA."[34] EMC appealed, arguing that "there was a disclosure or release of 'individually identifiable information,' but not medical information."[35] The Court of Appeal agreed with EMC.

The court found that "[i]t is clear from the plain meaning of the statute that medical information cannot mean just any patient-related information held by a healthcare provider, but must be 'individually identifiable information' and must also include 'a patient's medical history, mental or physical condition, or treatment.'"[36] The court next applied the rule against surplusage, and found that to consider information to be "medical information" whenever any kind of personally identifying information about a patient was released, would "render meaningless the clause 'regarding a patient's medical history, mental or physical condition, or treatment.'"[37] The court found that EMC's medical record number did not disclose anything about the nature of any medical treatment (if, in fact, treatment was provided) and that the fact that the person "was a patient is not in itself medical information as defined in section 56.05."[38] The court further held that "[c]onfirmation that a person's medical record exists somewhere is not medical information as defined under the CMIA."[39]

---

31 *Eisenhower Medical Center v. Superior Court* (Malanche), 226 Cal. App. 4th 430 (Cal. Ct. App. 2014).

32 *Id.*at 432.

33 *Id.* at 432-33.

34 *Id.* at 433.

35 *Id.* at 434.

36 *Id.* at 435 (citation omitted).

37 *Id.*

38 *Id.* at 435-36.

39 *Id.* at 436.

The court also found "noteworthy" the fact that section 56.16 of the CMIA allows an acute care hospital to release, at its discretion, certain limited patient information upon request, including a "general description of the reason for the treatment, the general nature of the injury, and the general condition of the patient, as well as nonmedical data."[40] Although the court acknowledged that section 56.16 applied only when there has been a request for information, it found that the section "does lend some support for the belief that the mere fact that a person is or was a patient is not accorded the same level of privacy as specific information about his medical history."[41] Finally, the court rejected the plaintiffs' contention that EMC's reporting of the theft to the HHS pursuant to the HIPAA data breach notification rule constituted an admission that the information was "medical information" because "federal law differs markedly from that in the CMIA."[42]

The court concluded by holding "that under the CMIA a prohibited release by a health care provider must include more than individually identifiable information but must also include information relating to medical history, mental or physical condition, or treatment of the individual."[43]

As to the flip side of the question, whether medical information that is disassociated from patient identifying information is encompassed by the CMIA, the plain language of the CMIA indicates that it is not, as the definition of "medical information" requires that the information include "individually identifiable information."[44] In 2014, this issue was addressed by the California Court of Appeal, Second Appellate District, which considered the propriety of disclosing medical information with patient information redacted.[45] In *Snibbe*, an orthopedic surgeon's postoperative orders were sought in discovery and the trial court ordered a limited production of a subset of those records, with patient identifying information redacted. The surgeon contended that while he had access to the records, he could not produce them without violating California privacy law, the CMIA and HIPAA. The Court of Appeal noted that patient privacy would not be violated when the surgeon failed to show that the postoperative orders could not be successfully redacted of patient identifying information.[46] In addition, the court noted that both the CMIA and HIPAA specifically provide exceptions for disclosure of medical information pursuant to court order.[47] As a result of the court order exception, the court did not directly rule on the issue of whether production of the redacted records would violate the CMIA. However, the court's general discussion of the lack of privacy violation when individually identifiable information is redacted, along with the plain language of the CMIA definition of "medical information" as including such information should preclude any such disclosures from violating the CMIA.

---

40 *Id.*

41 *Id.*

42 *Id.* at 436-37.

43 *Id.* at 437.

44 Cal. Civ. § 56.05(j).

45 *Snibbe v. Superior Court* (Gilbert), 224 Cal. App. 4th 184 (Cal. Ct. App. 2014), *review denied* (May 14, 2014).

46 *Id.* at 195-96.

47 *Id.* at 197-98. (citing Cal. Civ. § 56.10(b)(1) and 45 C.F.R. § 164.512(e)(l)(i)).

III. WHAT CONSTITUTES UNAUTHORIZED "RELEASE" OF MEDICAL INFORMATION UNDER THE CMIA?

Early CMIA cases typically involved the allegedly unauthorized intentional release of medical information (often to the employer of a plaintiff). In such cases, it was generally clear that the information had been "released" by the defendant. More recently, a number of CMIA cases have involved allegations of data breaches, such as through the theft of a computer or the potential exposure of information resulting from hacking into electronic medical records. In such cases, there has been considerable dispute regarding whether the circumstances of such a breach are sufficient to constitute a "release" of information under the CMIA. As described above, the CMIA obligates a provider of health care, health care service plan, pharmaceutical company or contractor to maintain "medical information . . . in a manner that preserves the confidentiality of the information contained therein," and any such party "who negligently . . . maintains, preserves, stores, abandons, destroys or disposes of medical information" is subject to specified remedies.[48] These remedies include nominal damages of $1,000 and/or actual damages from "any person or entity who has negligently *released* confidential information or records."[49]

The first published opinion to address the interpretation of the term "release" in the context of a data breach was *Regents of University of California v. Superior Court*, 220 Cal. App.4th 549 (Cal. Ct. App. 2013). In *Regents,* the Court of Appeal for the Second District considered the issue of whether there is a distinction between the terms "disclose" and "release" as used in the CMIA, and it held that although there is, the term "release" is to be broadly interpreted and does not require an affirmative act by a health care provider to state a claim under sections 56.101 and 56.36(b).[50] The *Regents* court held, however, that "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."[51] The court reasoned that because section 56.369(b) is incorporated into section 56.101(a), a plaintiff cannot bring a private cause of action for damages for violation of section 56.101 unless a "release" occurs.[52] The Court of Appeal further held that a no "release" of medical information would occur unless the plaintiff could demonstrate that her medical records were actually accessed, viewed or used by an unauthorized party."[53]

Likewise in *Sutter Health*, the California Court of Appeal, Third Appellate District, held that plaintiffs could not state a CMIA claim based on the theft of their medical records when they were unable to allege that the information was actually viewed by an unauthorized person.[54] Although the *Sutter Health* holding was similar to that in *Regents,* it was based on different grounds. The *Regents* court reasoned that allegations of theft of

48 Cal. Civ. § 56.101.

49 Cal. Civ. § 56.36(b) (emphasis added).

50 220 Cal. App. 4th 549, 564-69 (Cal. Ct. App. 2013).

51 *Id.* at 570.

52 *Id.* at 564.

53 *Id.* at 571 n. 15.

54 *Sutter Health v. Superior Court* (Atkins), 227 Cal. App. 4th 1546 (Cal. Ct. App. 2014).

a computer containing medical records were sufficient to state a claim for violation of section 56.101 (negligent maintenance of records), but found that the "release" of medical information triggering the remedy of $1,000 in nominal damages under section 56.36(b) could not be established without allegations that medical records were actually accessed, viewed or used by someone.[55] The court therefore held that because the standards of section 56.36(b) are incorporated into section 56.101, there could be no private right of action for violating section 56.101 unless a "release" occurred. In contrast, the *Sutter Health* ruling was based on the conclusion that no violation of section 56.101 itself could be established without alleging an actual viewing of the medical information.

In *Sutter Health*, patients brought a class action complaint alleging CMIA claims based on the theft of a computer containing medical records and seeking nominal damages for each class member, amounting to approximately $4 billion. The *Sutter Health* court ruled that plaintiffs had failed to establish a CMIA claim because they failed to allege that any unauthorized person actually viewed the medical records. The court first considered the legislative intent of the CMIA and noted that the requirements of section 56.101 were intended to protect the confidentiality of individually identifiable medical information, and that to violate the Act, "a provider of health care must make an unauthorized, unexcused disclosure of privileged medical information."[56] The court reasoned that "no breach of confidentiality takes place until an unauthorized person views the medical information," as it is the medical information, rather than the change in possession of the physical record, that is the focus of the Act.[57] The court explained that section 56.101 subjects health providers who "negligently" handle medical information to liability, that causation of injury is an essential element of negligence and that under the CMIA the required injury is a breach of confidentiality.[58] Applying this analysis to the allegations against Sutter Health, the court held that because the plaintiffs had not alleged an actual breach of confidentiality through the viewing of the information by an unauthorized party, Sutter Health's demurrer should have been sustained.[59] Finding that the plaintiffs had not demonstrated a reasonable possibility they could allege an actual breach of confidentiality, the court held that the action must be dismissed.[60]

Following *Regents* and *Sutter Health*, it is apparent that allegations of theft or loss of medical records, without more, are insufficient to establish a CMIA claim. For example, in *Falkenberg v. Alere Home Monitoring, Inc.*, No. 13-cv-00341-JST, 2014 WL 5020431, at *3 (N.D. Cal. 2014), which had been stayed pending the *Regents* and *Sutter Health* appeals, a federal district court dismissed plaintiffs' CMIA claims because the complaint failed to allege that confidential medical information stored on a stolen computer had been actually viewed by a third party. Although plaintiffs argued that a different plaintiff might be able to allege such facts, the court found that such argument did "nothing

55 *Regents*, 220 Cal. App. at 564, 571 n. 15.

56 *Sutter Health*, 227 Cal. App. 4th at 1557 (*citing Brown v. Mortensen*, 253 P.3d 522, 533-34 (Cal. 2011).

57 *Id.*

58 *Id.* at 1557-58.

59 *Id.* at 1558-59.

60 *Id.* at 1559.

to salvage the complaint."[61] Thus, under *Falkenberg*, unless a proposed CMIA class has at least one named plaintiff at the onset of an action who can allege that his or her information was actually viewed by a third party without authorization, the case will likely face dismissal at the pleading stage.

IV. CMIA ACTIONS FOR EMPLOYMENT DISCRIMINATION FOR FAILURE TO ALLOW ACCESS TO MEDICAL RECORDS

In addition to the CMIA's requirement that employers who obtain employee medical information handle it confidentially, as described above, the CMIA also provides that "[n]o employee shall be discriminated against in terms or conditions of employment due to that employee's refusal to sign an authorization [for release of medical information] under this part."[62] The California Supreme Court interpreted the prohibition and held that an employer's requirement for drug testing and disqualification of employees (and potential employees) who refused to authorize the physician conducting the test to release the results to the employer did not violate the CMIA.[63] In *Loder*, the California Supreme Court held that "[a]n employer 'discriminates' against an employee in violation of section 56.20, subdivision (b) if it improperly retaliates against or penalizes an employee for refusing to authorize the employee's health care provider to disclose confidential medical information to the employer or others"[64] However, the court did not characterize an employer's acts in disqualifying an employee or job applicant who refused to permit the employer to be informed of an employer-mandated medical examination or drug test to be discrimination, but rather found that such action was specifically authorized by section 56.20(b) as "necessary in the absence of medical information due to [the] employee's refusal."[65] The court noted that otherwise, any employer-mandated medical examination or drug testing procedure would be rendered "totally ineffective if an employer could not treat an individual who refuses to permit the employer to learn the ultimate results of the examination in the same fashion as an individual who refuses to complete the test."[66]

Employment discrimination under the CMIA was addressed again recently in *Kao v. Univ. of San Francisco*, 229 Cal.App.4th 437 (Cal. Ct. App. 2014), *review denied* (Nov. 25, 2014). In *Kao,* the plaintiff (formerly a tenured professor) was terminated after refusing to participate in a "fitness-for-duty examination" ("FFD") following various reports that his behavior had frightened other faculty members and school administrators.[67] Kao brought a CMIA claim (among others) in connection with his termination, alleging that he was fired for exercising his rights under the CMIA to refuse to release medical information.[68] The trial court instructed the jury that even "if Kao proved his refusal to

61 *Falkenberg*, 2014 WL 5020431 at *3.

62 Cal. Civ. § 56.20(b).

63 *Loder v. City of Glendale*, 927 P.2d 1200 (Cal. 1997), *cert. denied*, 52 U.S. 807 (1997).

64 *Id.* at 861.

65 *Id.*

66 *Id.*

67 229 Cal. App. 4th 437, 439-40 (Cal. Ct. App. 2014).

68 *Id.* at 452.

authorize release of confidential medical information for the FFD was 'the motivating reason for [his] discharge,' USF 'nevertheless avoids liability by showing that . . . its decision to discharge Kao was necessary because John Kao refused to take the FFD examination.'"[69] The Court of Appeal found that the evidence that supported findings that the FFD was job related and consistent with business necessity also supported a finding that his discharge was "necessary" within the meaning of Civil Code section 56.20, subdivision (b).[70] The court reasoned that because the university "unquestionably has a duty . . . to maintain a campus where people can safely work," and Kao's behavior was reported to frighten people and "cast a pall of 'fear and confusion' over the math department," the "jury could reasonably find that it was vital to the university's business to obtain an independent assessment of his fitness for duty."[71] The court therefore affirmed the judgment against Kao on his CMIA claim.

V. STANDING TO BRING A CMIA CLAIM

In CMIA cases, it is often difficult for plaintiffs to plead or prove that they have been harmed by the theft, loss or exposure of their medical information. Therefore such actions are often based on a theory that plaintiffs have been exposed to an increased risk of future harm as a result of the breach. In cases brought in federal court, defendants have opposed CMIA actions by challenging plaintiffs' Article III standing to bring a claim. In some cases, such challenges have been successful. For example, in *Whitaker v. Health Net of Cal., Inc.*, No. CIV S-11-0910 KJM-DAD, 2012 WL 174961 (E.D. Cal. 2012), a district court in the Eastern District of California held that plaintiffs failed to satisfy the injury-in-fact requirement when the only "injury" alleged was a health provider's loss of server drives containing plaintiffs' personal and medical information. The plaintiffs in *Whitaker* had contended that they had "standing because of the threat posed by the loss of their information."[72] The court reasoned that the "only allegation of particularized, real and immediate harm alleged" was plaintiffs' allegation "that one of them received a letter informing them their minor daughter's [s]ocial [s]ecurity number ha[d] been misused," and the daughter was not a member of the class.[73] Based on these allegations, the court held that plaintiffs' potential harm was "wholly conjectural and hypothetical" and that plaintiffs therefore lacked standing to bring their claims.[74] Plaintiffs in *Whitaker* had attempted to rely on two (non-CMIA) Ninth Circuit cases, *Krottner v. Starbucks Corp.*, 628 F.3d 1139 (9th Cir. 2010) and *Ruiz v. Gap, Inc., 380 F. App'x 689 (9th Cir. 2010),*[75]

---

69 *Id.* at 453.

70 *Id.*

71 *Id.* at 452 (citation omitted).

72 2012 WL 174961, at * 2.

73 *Id.* at *3.

74 *Id.* at *4.

75 The Ninth Circuit *Ruiz* opinion is unpublished and therefore not precedent in the Ninth Circuit. 9TH CIR. R. 36-3(a); *see also* FED. R. APP. R. 32.1.

which the *Whitaker* court found distinguishable.[76] Both of those Ninth Circuit cases involved the targeted theft of laptops from corporate businesses.[77]

In *Krottner,* one of the plaintiffs alleged that someone attempted to open a bank account in his name using his personal information following the theft.[78] "On these facts," the *Krottner* court found that the plaintiffs had "alleged a credible threat of real and immediate harm stemming from the theft of a laptop containing their unencrypted personal data."[79] In *Ruiz*, plaintiff "alleged, with support from an expert affidavit, that he was at a greater risk of identity theft."[80] The *Ruiz* plaintiffs' expert affidavit asserted that it was "substantially likely that the laptops were stolen for the Gap employee applicant data" [81] which was "easily accessible"[82] on the laptop. In fact, it appears that the *Ruiz* thief had to circumvent "multiple security measures" to gain access to the corporate facility and "passed by a number of other unsecured laptops in the same vicinity" to take a laptop that "was in the process of downloading the sensitive and personal information."[83]

The plaintiffs in *Whitaker* argued that there was "no difference between theft and loss" but the court held that "[e]ven if that is so, plaintiffs do not explain how the loss here has actually harmed them or threatens to harm them, or that third parties have accessed their data" and found their potential harm was too "conjectural and hypothetical" to support standing.[84]

Following *Whitaker*, similar standing arguments relying on "possible future harm" have been raised in a number of non-CMIA cases. In 2013, the United States Supreme Court issued a ruling in *Clapper v. Amnesty Int'l USA*, 133 S.Ct. 1138 (2013), which some defendants have attempted to use to limit *Krottner's* impact. In *Clapper,* attorneys and human rights, labor, legal and media organizations brought an action challenging a provision of the Foreign Intelligence Surveillance Act of 1978 [85] ("FISA"), and attempted to satisfy the Article III standing requirement based on their fear of impending future

---

76 *Whitaker*, 2012 WL 174961 at *2-*3.

77 The *Krottner* complaint alleged that "according to the Wisconsin Department of Agriculture, '[a] laptop containing personal information was stolen from the [Starbucks] corporate facility.'" Class Action Complaint at ¶ 16 *Krottner v. Starbucks Corp.*, 2009 WL 7382290 (W.D. Wash 2009) (No. 2:09-cv-00216-RAJ). And in *Ruiz*, the thief stole the laptop computers from the secured offices of a vendor who processed Gap job applications, bypassing other laptops to take those selected. Expert Report of Dr. Larry Ponemon at ¶¶ 3-4, attached as Ex. N to Rivas Decl. [Dkt.No.105-14], Ruiz v. Gap, Inc., No. CV07-05739-SC, filed November 13, 2007 (N.D. Cal.).

78 *Krottner*, 628 F.3d at 1142.

79 *Id.* at 1143.

80 *Ruiz*, 380 F. App'x at 691.

81 *Ruiz v. Gap, Inc.*, 622 F. Supp. 2d 908, 912-13 (N.D. Cal. 2009), *aff'd*, 380 F. App'x 689, 2010 WL 2170993 (9th Cir. 2010).

82 *Ruiz v. Gap, Inc.*, 540 F. Supp. 2d 1121, 1125 (N.D. Cal. 2008).

83 Expert Report of Dr. Larry Ponemon at ¶¶ 3-4, attached as Ex. N to Rivas Decl. [Dkt.No.105-14], *Ruiz v. Gap, Inc.*, No. CV07-05739-SC, filed Nov. 13, 2007 (N.D. Cal.).

84 *Whitaker v. Health Net of Cal., Inc.*, 2012 WL 174961, *2, *4 (E.D. Cal. 2012).

85 50 U.S.C. § 1801, *et seq.*

injury and the costs they incurred to avoid surveillance, among other things.[86] Plaintiffs alleged that parties to their communications were likely targets of FISA surveillance, that enactment of the provision interfered with their ability to obtain information and that they had "undertaken 'costly and burdensome measures' to protect the confidentiality of sensitive communications."[87] The Supreme Court found that the plaintiffs' theory of standing relied "on a highly attenuated chain of possibilities" and therefore did not satisfy the requirement that the threatened injury must be certainly impending.[88] In addition, the Court held that even if the injury requirement were established, the plaintiffs could not establish that any surveillance injury was traceable to the challenged provision, rather than another mechanism of surveillance.[89] Nor were plaintiffs able to prevail on the basis of measures they had implemented to avoid surveillance, as the Court found that such costs were not incurred to avoid a certainly impending harm, and that such costs suffered the same traceability defect.[90]

In 2014, a district court judge in the Southern District of California found that *Clapper* did not overrule or modify the Article III standard established in *Krottner.*[91] In *Sony Gaming,* plaintiffs brought an action based on allegations that hackers had accessed Sony's Network and stolen sensitive personal information (including credit card numbers and codes, login information, birth dates, etc.) of millions of customers, and that Sony delayed in notifying its customers of the breach.[92] Sony argued that the allegations were insufficient to establish standing, but the court found that plaintiffs had "plausibly alleged a 'credible threat' of impending harm based on the disclosure of their [p]ersonal [i] nformation following intrusion."[93] Similarly, in *In re Adobe Systems, Inc. Privacy Litigation*, No. 13-CV-05226-LHK, 2014 WL 4379916 (N.D. Cal. 2014), a district court in the Northern District of California held that the plaintiffs' allegations that hackers deliberately targeted Adobe's servers and spent several weeks collecting personal data, including usernames and passwords and credit card numbers and expiration dates, and that some of the stolen data had already surfaced on the internet, satisfied standing requirements of both *Krottner* and *Clapper.* The court noted that under those circumstances, there was "no need to speculate" as to whether plaintiffs' information had been stolen, whether the hackers intended to misuse the stolen information or whether they would be able to do so.[94] The court noted that the danger that the stolen information would be misused could "plausibly be described as 'certainly impending'" and that the threatened injury could

---

86 *Clapper,* 133 S.Ct. at 1145-46.

87 *Id.*

88 *Id.* at 1148.

89 *Id.* at 1149.

90 *Id.* at 1151-52.

91 *In re Sony Gaming Networks and Customer Data Security Breach Litigation*, 996 F. Supp. 2d 942, 961 (S.D. Cal. 2014).

92 *Id.* at 955.

93 *Id.* at 962.

94 *In re Adobe Systems*, 2014 WL 4379916, at *8.

only be more imminent if the allegations had stated that the information had already been misused.[95]

In contrast, when allegations of harm are more remote, courts have declined to find standing. For example, in *Yunker v. Pandora Media, Inc.*, No. 11-CV-03113 JSW, 2013 WL 1282980, at *5 (N.D. Cal. 2013), the court found that Yunker's allegations of potential future harm were insufficient to establish standing. In that case, the plaintiff claimed violations of the UCL and various privacy laws based on allegations that defendant did not anonymize his personal information (consisting of his age, gender, location and user id), even though it represented that it would, and further permitted advertising libraries to access the personal information.[96] The court found the case distinguishable from *Krottner* because Yunker did not allege the disclosure of sensitive financial information, such as a social security number or a credit card number, nor had he "alleged that anyone has breached Pandora's servers."[97] The court found that allegations that the information was provided to advertising libraries were insufficient to establish standing, in that "at best" such factual allegations "show it might be possible that, in the future, he could be the victim of identity theft," and that the possibility of future harm was "insufficient to establish standing."[98] Likewise, in the *In re Google, Inc. Privacy Policy Litigation*, No. 5:12-CV-01382, 2014 WL 3707508, at *6 (N.D. Cal. 2014), a district court held that allegations of risk of future harm from the unauthorized disclosure of commingled user data, such as account information with search queries, was too conjectural to satisfy standing requirements. The court distinguished the case from *Krottner,* as the disclosure there "was a result of laptop theft containing sensitive personal information of almost 100,000 Starbucks employees," and further noted that in *Google* no criminal activity was alleged.[99]

Thus far, it is unclear how significant an impact *Clapper* will have on the Article III standing threshold for privacy cases. Based on the recent cases discussed above, breaches that appear to be targeted and deliberate attempts to access the personal data at issue, such as in *Krottner, Sony Gaming,* and *Adobe,* may be more likely to lead to allegations that satisfy the Article III standing requirement. In contrast, for incidents in which the data is potentially available for access but there is no evidence of theft, such as *Google, Yunkers,* or *Whitaker* (or potentially in theft cases in which there is nothing to suggest that personal information is the target of the theft, such as random equipment theft),[100] there may not be sufficient allegations to establish standing to bring an action. In addition, in a number of cases it appears that the standing analysis was impacted by the sensitivity

95 *Id.*

96 *Yunker*, 2013 WL 1282980, at *1.

97 *Id.* at *5.

98 *Id.*

99 *In re Google*, 2014 WL 3707508, at *6.

100 *See, e.g., In re Science Applications Int'l Corp. (SAIC)*, No. 12-347 JEB, 2014 WL 1858458 (D.C. 2014) (dismissing privacy claims of most plaintiffs based on allegations of theft of personal information on several data tapes stolen from an employee's car along with a GPS system and stereo on the grounds that mere loss of data is insufficient to confer standing, but finding that two plaintiffs plausibly alleged that their data was accessed or abused when personal information similar to that contained on the tapes was misused).

of the information stolen or lost–the more sensitive the information and more likely to lead to damages, the more likely that standing will be found. With respect to medical information, one might argue that it is all sensitive, but even so, there would likely be substantial variation in the sensitivity of the types of data at issue (e.g., record of sexually transmitted disease versus record of a dermatologist visit). In addition, with the recent decisions in *Sutter Health* and *Regents,* the standing argument may have less significance in CMIA cases, as the standards for bringing such an action now appear higher than those for establishing standing. However, Article III standing may still be a viable issue in any medical information breach action that is brought under other privacy laws.

VI. OTHER CALIFORNIA PRIVACY PROVISIONS TARGETED AT MEDICAL INFORMATION

There are a number of other relevant laws targeting the confidentiality of California residents' medical information.

Health and Safety Code section 1280.15(a): This section requires that certain clinics, health facilities, home health agencies and hospices "shall prevent unlawful or unauthorized access to, and use or disclosure of, patients' medical information" and establishes an administrative penalty of up to $25,000 per patient, and up to $17,000 per each subsequent occurrence of unlawful or unauthorized access, use or disclosure of the patient's medical information.[101] In addition, the health care providers subject to this statute must notify the California Department of Public Health ("CDPH") and all affected patients (or their representatives) within fifteen days of the breach (unless asked not to do so by law enforcement).[102] Violations of the disclosure requirement are subject to administrative penalties of up to $250,000 per incident (in combination with those authorized in subsection (a)).[103] The CDPH relies on this provision to allow it to evaluate breaches of confidentiality and seek penalties on an ongoing basis.[104] In addition to its use by the CDPH, because the statute adopts a slightly different formulation from that of the CMIA (as it specifically prohibits unauthorized access), section 1280.15 has been used to target unauthorized activities of health care employees.[105]

Health and Safety Code section 1280.18(a): This section requires that "[e]very provider of health care shall establish and implement appropriate administrative, technical, and physical safeguards to protect the privacy of a patient's medical information" and "shall reasonably safeguard confidential medical information from any unauthorized access or unlawful access, use, or disclosure."[106] The CDPH may assess administrative fines against any person or provider of health care for any violation of section 1280.18 or of the CMIA,

---

101 Cal. Health & Safety § 1280.15(a).

102 *Id.* § 1280.15(b),(c).

103 *Id.* § 1280.15(d).

104 *See, e.g.*, List of Penalties, Cal. Dept. of Pub. Health, http://www.cdph.ca.gov/ (search site for "breach of confidentiality" for a list of penalties issued by year).

105 *See, e.g., Scholink v. Salinas Valley Memorial Healthcare System*, No. H040057, 2014 WL 6991708, at *3 (Cal. Ct. App. 2014).

106 Cal. Health & Safety § 1280.18(a).

in the same amount as provided in Civil Code section 56.36.[107] The provision allowing for fines does not apply to clinics, health facilities, home health agencies and hospices subject to section 1280.15, above.[108]

California Civil Code section 1798.81.5: This section requires businesses that own, license, or maintain "personal information" (which includes, among other things, a subset of "medical information" subject to the CMIA)[109] about California residents to "implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."[110] In addition, these businesses must require that any contractors to which they disclose such information agree by contract to maintain such security procedures and practices.[111] As noted above, if these businesses are also either "organized for the purpose of maintaining medical information" or offer "software or hardware to consumers, including a mobile application or other related device that is designed to maintain medical information" (e.g., personal health record vendors), they are also deemed to be "provider[s] of health care" for the purpose of subjecting them to the CMIA.[112] However, while other "provider[s] of health care" under CMIA are exempt from the security requirements of section 1798.81.5,[113] that exemption does not apply to such personal health record vendors and others.[114]

California Civil Code section 1798.82: This is California's data breach reporting law, which includes "medical information" within the definition of "personal information" when accompanied by "[a]n individual's first name or first initial and last name" if one or the other is not encrypted.[115] Pursuant to section 1798.82(a), a business or state agency must notify any California resident whose unencrypted personal information, as defined, was acquired, or reasonably believed to have been acquired, by an unauthorized person. In addition, pursuant to section 1798.82(g), a person or business that is required to issue a security breach notification to more than 500 California residents as a result of a single breach of the security system is required to electronically submit a copy of the security breach notification, excluding any personally identifiable information, to the Attorney General.

California Civil Code section 1798.91: This section prohibits a business from seeking to obtain medical information from an individual for direct marketing purposes without, (1) clearly disclosing how the information will be used and shared, and

---

107 *Id.* § 1280.17(a)(1).

108 *Id.* § 1280.17(a)(2).

109 CAL. CIV. § 1798.81.5(d)(2) defines "medical information" as "any individually identifiable information, in electronic or physical form, regarding the individual's medical history or medical treatment or diagnosis by a health care professional."

110 *Id.* § 1798.81.5(b).

111 *Id.* § 1798.81.5(c).

112 *Id.* §§ 56.06(a), (b).

113 *Id.* § 1798.81.5(e)(1).

114 *Id.* §§ 56.06(a),(b).

115 *Id.* § 1798.82.

(2) getting the individual's consent.[116] If information is requested orally, an audio recording of the consent must be retained for two years after the conversation.[117] This section is distinguishable from the CMIA in that it does not apply to a provider of health care, health care service plan, or contractor as defined in Civil Code section 56.05.[118] This section has not been heavily relied on in litigation, perhaps because of difficulties associated with establishing any injury resulting from violations.

California Health & Safety Code section 120980: This section imposes civil penalties upon the negligent or willful and malicious disclosure of the results of an HIV test to any third party in a manner that identifies or provides identifying characteristics of the person to whom the test results refer, and provides for the possibility of criminal sanctions if the disclosure results in economic, bodily, or psychological harm to that person.[119] There are exceptions to this rule, including one permitting the physician who ordered the test to include the result in the patient's medical record and then to disclose that medical record to certain providers of care, for the purposes of diagnosis, care, or treatment.[120]

California Welfare and Insurance Code section 5328 of the Lanterman-Petris-Short ("LPS") Act: This section contains a confidentiality provision protecting "information and records obtained in the course of providing services" relating to voluntary and involuntary mental health assessment and treatment.[121] Section 5328 *et seq.* provide detailed restrictions on the disclosure of records, limiting who, and for what purposes, information may be disclosed and detailing the consent process for various types of disclosures.[122] Disclosure of information in violation of section 5328 is actionable under California Welfare and Insurance Code section 5330, which provides that "any person" may bring an action for damages for release of his or her confidential information in violation of the LPS Act for: (1) the greater of $10,000 or treble damages if the release was willful and knowing; or (2) for both $1,000 in statutory damages (without requiring a showing of actual damages) and the amount of actual damages for negligent release.[123] A plaintiff may also recover court costs and reasonable attorney's fees.[124]

VII. UNFAIR COMPETITION LAW CLAIMS

In addition to CMIA claims, some plaintiffs have asserted claims under the UCL associated with alleged losses or theft of medical information. To state a claim under the UCL, a plaintiff must demonstrate that some business act or practice is either "unlawful,

---

116 *Id.* § 1798.91(c).

117 *Id.* § 1798.91(b)(2).

118 *Id.* § 1798.91(d).

119 Cal. Health & Safety § 120980.

120 *Id.* § 120980(l).

121 Cal. Welf. & Inst. § 5328.

122 *Id.* §§ 5328.01-5328.06.

123 *Id.* § 5330(a), (b).

124 *Id.* § 5330(d).

unfair or fraudulent."[125] In *California Consumer Health Care Council v. Kaiser Foundation Health Plan, Inc.,*[126] a plaintiff sued Kaiser, alleging that its practice of transmitting allegedly "irrelevant" medical information to its attorneys concerning Kaiser patients who had brought, or might be contemplating, medical malpractice claims against Kaiser violated the UCL. The plaintiff alleged that Kaiser "engaged in the following practices: (1) 'disclosing medical information regarding patients without first obtaining such patient's authorization or otherwise being authorized to do so under the law'; (2) 'sharing, selling or otherwise using medical information regarding such patients for a purpose not necessary to provide health care services to the patients'; and (3) 'concealing' these practices from patients."[127] These actions allegedly violated the UCL under all three prongs as it was: (1) unlawful because Kaiser violated the CMIA and rights to privacy under the California Constitution; (2) unfair because the harm to patients outweighs the "utility" of Kaiser's acts; and (3) fraudulent and misleading because Kaiser represented that it used and disclosed patient medical information only in accordance with the law.[128] The court held that the alleged practices were not unlawful under the UCL because the disclosure fell within an exception to the CMIA permitting disclosure to persons responsible for defending professional liability claims for Kaiser, and that the exception did not exclude "irrelevant" information.[129] The court likewise held that plaintiff's constitutional privacy claim failed because she did not have a reasonable expectation of privacy in light of the CMIA exception, and because a patient signaling an intent to bring a malpractice claim cannot reasonably expect his or her information to be kept from the health care provider's attorneys.[130] In addition, the court found that the UCL claim was precluded by the injury requirement of section 17200, as the plaintiff was a public interest organization and did not allege that it was authorized to represent any Kaiser patient who had been or was likely to be injured by the policy.[131]

More recently, plaintiffs brought a UCL claim in *Falkenberg v. Alere Home Monitoring, Inc.,*[132] which was denied for lack of standing. In *Falkenberg*, the plaintiffs' UCL claim was based on the theory that the theft of an employee's laptop containing confidential medical information resulted in lost money or property consisting of "expenditures on credit monitoring, increased risk of identity theft, and expenditures made to Defendant based on the reasonable expectation that Defendant would maintain the privacy of the personal and medical information of the Plaintiffs and the class."[133] The court first characterized the injury requirement under the UCL (loss of money or property) as "more stringent than the federal Article III standing requirement, [which] 'may be intangible and need

125 Cal. Bus. & Prof. § 17200.

126 42 Cal. App. 4th 21 (2006).

127 *Id.* at 25-26.

128 *Id.* at 26.

129 *Id.* at 28 (citing Cal. Civ. § 56.10(c)(4)).

130 *Id.* at 32.

131 *Id.* at 33-34.

132 No. 13-cv-00341-JST, 2014 WL 5020431 (N.D. Cal. Oct. 7, 2014).

133 *Id.* at *4.

not involve lost money or property' . . . ."[134] The court then compared the claim to that brought in *Ruiz v. Gap, Inc.,*[135] which was based on allegations that plaintiffs lost property when their confidential personal information was contained on stolen laptops.[136] The court noted that in *Ruiz*, the plaintiffs failed to present "any authority to support the contention that unauthorized release of personal information constitutes a loss of property," and noted that same was true in *Falkenberg*, "finding that in the absence of any such authority, Plaintiffs have not alleged any loss of property."[137] The court also found that while the plaintiffs claimed to have expended money on credit monitoring, the defendant had offered one year of credit monitoring to all plaintiffs, thus "[w]ithout specifically identifying what expenditures were necessary in excess of this offer, Plaintiffs cannot establish what money was lost."[138]

Because of the high potential damages associated with the CMIA, in contrast to the equitable remedies available under the UCL, UCL claims have not typically been a primary means for seeking relief in medical information breach cases. In addition, the injury requirement makes UCL actions challenging, as it may be difficult to tie any particular financial injury to the lost or stolen information. Consequently, for a UCL claim to survive in a medical information loss, theft or breach case, plaintiffs will need to allege sufficient facts to establish exactly what money or property was lost and how such a loss "resulted from" the alleged breach.

VIII. UNRESOLVED ISSUES AND FUTURE TRENDS

Violations of Notice Requirements

The CMIA does not contain its own notice requirement in the event of a data breach, but disclosures encompassed by the CMIA remain subject to the notification provisions of California Civil Code section 1798.82(d).[139] The disclosure is required to be made "in the most expedient time possible" (with exceptions for delay due to law enforcement agency requirements for a delay so as not to impede an investigation).[140] In addition to the notification, when the notifying party was the source of the breach it must also offer to provide appropriate identity theft prevention and mitigation services for at least 12 months if the information exposed (or that may have been exposed) included a social security or California driver's license or identification card number and an individual's last name, with first name or initial, and either the names or data elements were not

---

134 *Id.*

135 540 F. Supp. 2d 1121, 1125 (N.D. Cal.2008), *aff'd*, 380 Fed.Appx. 689 (9th Cir. 2010).

136 *Falkenberg*, 2014 WL 5020431, at *4

137 *Id.* (quoting *Ruiz*, 540 F. Supp. 2d at 1127).

138 *Id.*

139 Cal. Civ. § 1798.82(d). In contrast, covered entities and business associates subject to HIPAA that comply with the notice requirements under the HIPAA Data Breach Notification (section 13402(f) of the Federal Health Information Technology for Economic and Clinical Health Act) are deemed to have complied with the disclosure requirements of California Civil Code section 1798.82(d), but not the statute's other requirements such as identity theft protection, if applicable. 45 C.F.R. § 164(D).

140 *Id.* § 1798.82(a), (c).

encrypted.[141] In many cases, when lawsuits are filed after notification, they target not only laws prohibiting disclosure, but also violations of the notification requirements, such as unreasonable delay, or insufficient compliance with the content requirements for notice. California Civil Code section 1798.84(b) provides that "any customer injured by a violation of this title may institute a civil action to recover damages."[142]

It is possible that an identity theft type of injury could occur from defects in the notice procedure or timing (*e.g.*, identity theft occurred after breach was identified but before compliant notice was sent and harm therefore might have been prevented absent the notice defects). However, in most cases, this type of injury is not alleged, or cannot be established. Rather, plaintiffs may attempt to satisfy the "injury" requirements by pleading an "informational injury": essentially, that injury resulted from not receiving information to which affected persons are statutorily entitled. Plaintiffs have not met with much success in raising this argument in California. In *Boorstein v. CBS Interactive, Inc.,*[143] the most recent published decision addressing the requirement for "injury" under section 1798.84 in the context of violations of California's Shine the Light Law[144] (requiring certain disclosures upon customer request when personal information has been disclosed and used by third parties for marketing purposes), the court held that no California cases recognize the "informational injury" the plaintiff allegedly suffered.[145] However, in that case the plaintiff had not requested the informational notice, as required by the statute, and so the situation would not be identical to an alleged violation of section 1798.82(d), in which notice is required without any action by the persons affected. Thus, although the "informational injury" argument has not succeeded in any Shine the Light case applying section 1798.84 following *Boorstein*, it is unclear whether a successful argument could potentially be made in asserting violations of section 1782(d).[146]

Other Potential Covered Parties

In 2013 (effective January 1, 2014), the CMIA was amended to clarify its application to personal health record ("PHR") vendors.[147] The emergence of various internet-based businesses offering patients their own means of storing and managing their medical information, often through mobile applications, raised privacy concerns in the legislature.[148] Although certain businesses organized for the purposes of maintaining

---

141 *Id.* § 1798.82(d)(2)(g).

142 *Id.* § 1798.84(b).

143 165 Cal. Rptr. 3d 669 (Cal. App. Ct. 2013).

144 Cal. Civ. § 1798.83.

145 Boorstein, 165 Cal. Rptr. 3d at 679-681.

146 *See, e.g., Baxter v. Rodale, Inc.*, 555 Fed. Appx. 728 (9th Cir. 2014) (plaintiff failed to state a claim); *Murray v. Time Inc.*, 554 Fed. Appx. 654 (9th Cir. 2014) (dismissed for lack of standing); *King v. Conde Nast Publications*, 554 Fed. Appx. 545 (9th Cir. 2014) (dismissed for lack of standing); *Miller v. Hearst Communications Inc.*, 554 Fed. Appx. 657 (9th Cir. 2014) (dismissed for lack of standing). All of these decisions are unpublished.

147 A.B. 658, chap. 296, 2013 Leg. (Cal. 2013), amending Cal. Civ. § 56.06(b); *see also* Analysis of Assembly Judiciary Committee of A.B. 658, at 1 (Cal. Apr. 15, 2013).

148 A.B. 658, chap. 296, 2013 Leg. (Cal. 2013); Analysis of Assembly Judiciary Committee, at 1,3 (Cal. Apr. 15, 2013).

medical information have been subject to the CMIA since 1993, the amendment was intended to ensure that the CMIA would apply to all PHR vendors that maintain medical information, including through mobile applications provided to patients, whether or not the business was organized for that purpose.[149]

During the legislative process, industry representatives expressed a concern that the amendment be clearly defined so as not to encompass those businesses that maintain personal health information generated directly by consumers, such as personal fitness information.[150] Because "medical information" is defined under the CMIA as limited to information "*in possession of or derived from* a provider of health care, health care service plan, pharmaceutical company, or contractor"[151] information contributed by a patient directly would not appear to be encompassed.[152] However, the bill's author addressed the concern by clarifying that the provisions added by the bill only apply to medical information that originates with a health care provider, health care service plan, or medical contractor.[153] The final amendment limited the covered businesses to those offering "software or hardware to consumers, including a mobile application or other related device that is designed to maintain medical information."[154]

As health monitoring equipment and applications become increasingly advanced, and the level of personal health information maintained by non-health care entities increases, it is likely that ongoing privacy concerns about health information created by an individual will prompt future legislation. Currently, personal fitness data is distinguished from covered medical information on the ground that personal fitness data is not in the hands of, or coming from, specific types of health care providers. As technology continues to develop and transfer of electronic health information between patients and health care providers becomes more common, it may become increasingly difficult to maintain the distinction between information possessed by, or derived from, health care providers and that generated by a patient. Future legislation may potentially be initiated to increase protections on personal fitness data, whether through modification of the CMIA or by bolstering California's other privacy protection statutes, such as Civil Code section 1798.81.5, which already requires implementation of "reasonable security procedures and practices" for protecting Californians' personal information which is

149 *Id.*

150 A.B. 658, chap. 296, 2013 Leg. (Cal. 2013); Analysis of Assembly Committee on Judiciary, at 4 (Cal. Apr. 15, 2013).

151 "Contractor" means any person or entity that is a medical group, independent practice association, pharmaceutical benefits manager, or a medical service organization and is not a health care service plan or provider of health care. "Contractor" does not include insurance institutions as defined in subdivision (k) of Section 791.02 of the Insurance Code or pharmaceutical benefits managers licensed pursuant to the Knox-Keene Health Care Service Plan Act of 1975 (Chapter 2.2 (commencing with Section 1340) of Division 2 of the Health and Safety Code). Cal. Civ. § 56.05(d).

152 Cal. Civ. § 56.05(j) (emphasis added).

153 Cal. Civ. § 56.06(b), citing Cal. Civ. § 56.05(j); *see also* A.B. 658, chap. 296, 2013 Leg. (Cal. 2013); Analysis of Assembly Judiciary Committee, at 4 (Cal. Apr. 15, 2013).

154 Cal. Civ. § 56.06(b).

defined to include "medical information."[155] The term "medical information" under section 1798.81.5 is defined as "any individually identifiable information, in electronic or physical form, regarding the individual's medical history or medical treatment or diagnosis by a health care professional."[156] Privacy rights organizations may seek to expand that definition in the future to include information regarding a person's physical condition. Currently, Civil Code section 1798.81.5(e) specifically excludes entities regulated by the CMIA and HIPAA.

The Treatment of Patient Lists From Specialized Health Care Providers

Although one California Court of Appeal (in *Eisenhower*) has held that release of individually identifying information relating to patients, when divorced from any specific medical information, is not actionable, many important issues remained unresolved.[157] For example, the *Eisenhower* decision expressly declined to address whether the fact that a person was a patient of a particular healthcare provider, such as a physician whose specialty might be readily determined, or a specialized facility such as an AIDS clinic, may rise to the level of medical information.[158] There are numerous other situations where this issue could arise, for example, infertility clinics, obesity treatment clinics, sleep disorder centers, mental health facilities, etc. Likewise, depending on the nature of a physician's specialty, the disclosure of a patient's name associated with a particular physician might be considered disclosure of healthcare information. While these issues have not yet been resolved, healthcare providers and others subject to the CMIA are well advised to treat patient lists as confidential and protect them against disclosure.

Vendor Disclosure Issues

Under the CMIA, information may be disclosed to certain contractors and service providers. In fact, many health care providers rely heavily on third-party vendors for data processing, billing or other administrative services. Under the HIPAA Privacy Rules, covered entities and business associates may be held liable under certain circumstances for the acts of their agents,[159] but it remains unclear the extent to which health care providers will be held liable under the CMIA for the breaches of their vendors. In addition, unlike HIPAA, which has established a specific "minimum necessary standard" that applies to uses and disclosures of protected health information by covered entities and their business associates,[160] the standards for disclosure under the CMIA are less clear. For example: (1) "information may be disclosed to providers of health care, health care service plans, contractors, or other health care professionals or facilities *for purposes of diagnosis or treatment of the patient*"; (2) "information may

155 Cal. Civ. §§ 1798.81.5(b), 1798.81.5(d)(1).

156 *Id.* § 1798.81.5 (d)(D)(2).

157 *See, e.g., Eisenhower Medical Center*, 172 Cal. Rptr. 3d 165 (Cal. App. Ct. 2014) (holding that patient lists do not constitute medical information); *Maureen K v. Tuscka, M.D.*., 155 Cal. Rptr. 3d 620 (Cal. App. Ct. 2013) (holding that description of patient's medical history without information revealing the patients identity did not violate CMIA).

158 *Eisenhower*, 172 Cal. Rptr. 3d at 171, n.3-4.

159 45 C.F.R. § 160.402(c).

160 45 C.F.R. §§ 164.502(b), 164.514(d).

be disclosed to an insurer, employer, health care service plan [etc.] *to the extent necessary to allow responsibility for payment to be determined and payment to be made*"; and (3) "information may be disclosed to a person or entity that provides billing, claims management, medical data processing, or other administrative services" seemingly without qualification.[161] Future cases may help clarify disclosure limitations and liability under the CMIA with respect to its relationship to third-party vendors.

Class Certification

The potential release of medical information, whether occurring through improper disposal of records, computer hacking or theft, frequently involves mass data. However, there has yet to be any published decision in which a CMIA class has been certified. Following the decisions in *Regents and Sutter*, such certification appears increasingly unlikely – at least for those classes based on theft of information. Under current law, the CMIA now requires that plaintiffs plead and prove that their medical information was actually viewed by an unauthorized individual. For cases involving physical thefts, such as those of computers, drives or disks, such viewing will likely be difficult to establish unless the thief is identified and his viewing of the information can somehow be confirmed. For instances of hacking, there may be an electronic record of viewing, but problems may still exist at the class certification phase. As in many other types of privacy-related actions, even if a class member's information is viewed, there may be difficulties associated with establishing that any harm resulted from the viewing. Even if one or more members of a putative class experiences misuse of their personal or medical information, it may be difficult to establish a correlation between the theft or breach and any privacy-related injury. In this era of pervasive electronic presence, many people have had their information disclosed through a wide variety of data breaches and/or through self-disclosure. Any named plaintiff will likely be scrutinized closely for individualized issues associated with his or her data history. In addition, it has yet to be determined the extent to which each class member will have to establish that his or her information was viewed, which could potentially defeat class certification. In instances of data breaches involving millions of individuals, it would appear unlikely that all data would be uniformly accessed and viewed.

Plaintiffs seeking class certification also may encounter limitations in obtaining information from potential class members to support certification arguments, as even disclosure of putative class member names may be limited, depending upon the nature of the class. If the putative class is one which is identified by inclusion in specific health provider records, such as those of an infertility or weight loss clinic or a particular physician, medical information about the patient may arguably be inferred from the class list, and the court may preclude provision of patient lists to plaintiff's counsel. For example, in one non-CMIA case, the California Court of Appeal, Second Appellate District, held that in a class action case involving patients who received incorrect medication for syphilis, constitutional rights to privacy prohibited disclosure of the putative class members' names and addresses to class counsel without affirmative consent.[162] The court

161 Cal. Civ. § 56.10(c) (emphasis added).

162 *Los Angeles Gay and Lesbian Center v. Superior Court* (Bomersheim), 125 Cal. Rptr. 3d. 169 (Cal. Ct. App. 2011).

held that "no class members' name, identifying information or medical information is to be disclosed without that class members' [sic] prior authorization," and that the trial court must "take steps to ensure that the names, identifying information, and medical information of the class members are not subject to disclosure under any circumstances in any public proceeding or public filing."[163] Although names and contact information for class members may not necessarily require the same level of protection in all CMIA cases, this case illustrates that contacting putative class members in some circumstances (e.g., when the nature of the class itself discloses personal health information) in order to obtain information to assist with class certification may be challenging. Even though solutions may be found, such as through coding or redacting information, these methodologies impose additional burden and cost.

IX. CONCLUSION

Barring dramatic advances in technology or human behavior, data breaches involving medical information should be expected to continue to pose serious risks. Although recent decisions in the California Court of Appeal have made it more difficult for class action plaintiffs to pursue lawsuits against health care providers and others that sustain breaches of medical information, California law continues to make special demands upon those that create or receive, or use, disclose, or maintain, medical information. Some of these demands go beyond what may be required of those parties under HIPAA and apply to a number of parties that are not subject to HIPAA. While those who work with medical information may welcome the limited protection from lawsuits that these recent court cases offer, it will remain important to stay abreast of future developments, both in the legislature and in the courts, regarding this rapidly evolving subject.

163 *Id.* at 186.