Advisory

pillsbury

Privacy, Data Security & Information Use | Cybersecurity Task Force | Litigation | Health Care

July 8, 2014

California Court Limits Liability for Loss of Certain Patient Information under CMIA

By Joseph R. Tiffany, Connie J. Wolfe, Ph.D., and Allen Briskin

California appellate courts are clarifying potential liability under California's Confidentiality of Medical Information Act, Cal. Civ. Code § 56 et seq. *("CMIA") of health care providers, health plans, pharmaceutical companies and others for the unauthorized disclosure of medical information. The CMIA provides that an individual may recover $1,000 nominal damages (plus actual damages if any) from a health care provider or other covered party that negligently releases that individual's medical information. In data breaches involving large numbers of records and individuals, the potential liability can be enormous even without proof of any damages.*

Eisenhower Medical Center Case

In a significant decision for health care providers and other holders of medical information, the California Court of Appeal recently decided that the CMIA's civil liability provisions do *not* cover the theft of a hospital index containing personal identifying information *unless* the index also includes information relating to medical history, mental or physical condition, or treatment. *Eisenhower Medical Center v. Superior Court (Malanche)*, No. E058378, 2014 WL 2115216, at *1 (Cal. Ct. App. May 21, 2014). In *Eisenhower*, the plaintiffs sought damages for a class of over 500,000 individuals, which could amount to total nominal damages of over $500 million without any showing of actual injury. While the CMIA continues to impose significant obligations upon those within its coverage, this decision dramatically reduces the liability risk arising from the release of one type of information.

Under the CMIA, a provider of health care, health care service plan, pharmaceutical company or contractor is obligated 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. Cal. Civ. Code § 56.101. Such remedies include nominal damages of $1,000 and/or actual damages from "any person or entity who has negligently released confidential information or records...." Cal. Civ. Code § 56.36(b). The CMIA defines the term "medical information" as follows:

> "Medical information" means 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.

Cal. Civ. Code § 56.05(j).

In *Eisenhower*, 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.

Prior to *Eisenhower*, the California Court of Appeal had held that the term "medical information" as used in 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.'" *Garrett v. Young*, 109 Cal. App. 4th 1393, 1406 (2003). The Court of Appeal had also ruled that a valid claim of improper disclosure of "medical information" required that the information about an individual's health condition be accompanied by specific information that identified the individual involved. *Maureen K. v. Tuschka, M.D.*, 215 Cal. App. 4th 519 (2013) (holding there was no disclosure of any identifying medical information where physician discussed patient's HIV-positive condition in a room containing other patients, but did not use plaintiff's full name, or disclose any other identifying information specified in the statute, and that there was no evidence that other patients would have been able to see the plaintiff during the discussion).

The *Eisenhower* decision takes the analysis one step further, and holds that "medical information" under the CMIA (*i.e.*, information "regarding" a patient's medical history, condition, or treatment) must include or reveal something about the patient's history, condition, or treatment. A computer was stolen that contained an index of over 500,000 persons to whom the Eisenhower Medical Center ("EMC") had assigned a clerical record number and that included each person's name, medical record number, age, birth date, and the last four digits of their Social Security number. 2014 WL 2115216 at *1. The computer was password-protected but not encrypted. EMC argued "that the index did not contain medical information within the meaning of the CMIA," and that "there was a disclosure or release of 'individually identifiable information,' but not medical information." *Id*. The Court of Appeal agreed.

The Court first looked at the wording of the CMIA, and 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 also include 'a patient's medical history, mental or physical condition, or treatment." *Id*. at *3. The Court next found that plaintiff's theory would require information to be considered "medical information" whenever any kind of personally identifying information about a patient was released, "render[ing] meaningless the clause 'regarding a patient's medical history, mental or physical condition, or treatment." *Id*. The Court found that the 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." *Id*. at *4. The Court further held that "[c]onfirmation that a person's medical record exists somewhere is not medical information as defined under the CMIA." *Id*.

The Court found it "noteworthy" 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." *Id*. Although the Court acknowledged that section 56.16 applies 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." Finally, the Court rejected plaintiffs' contention that EMC's reporting of the theft to the U.S. Department of Health and Human Services pursuant to federal law constituted an admission, finding that because "federal law differs markedly from that in the CMIA," the provision did not constitute a concession that the theft involved medical information as defined in the CMIA. *Id*.

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." *Id*.

Although *Eisenhower* is significant for its clarifications regarding the definition of medical information, the *Eisenhower* Court expressly declined to address other important issues relating to interpretation of the CMIA: (1) whether there is a distinction between a disclosure or release of medical information under the CMIA; and (2) whether the very fact that a person was a patient of certain health care providers, such as an AIDS clinic, may rise to the level of medical information. *Id*. at *2 n.3, *4 n.4.

Unresolved Issues after *Eisenhower*

Thus far, only the Court of Appeal for the Second District has 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). *Regents of University of California v. Superior Court*, 220 Cal. App. 4th 549, 564-69 (2013). However, that Court held 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." *Id*. at 570. Instead, "[w]hat is required is pleading, and ultimately proving, that the confidential nature of the plaintiff's medical information was breached as a result of the health care provider's negligence." *Id*. The Court of Appeal therefore held that the medical provider's demurrer should have been sustained without leave to amend, and the case dismissed, when plaintiff failed to allege that her medical records were actually accessed, viewed or used by anyone, and could offer only "minimal facts" that would require "too many layers of speculation" "to be considered sufficient to overcome the deficiency in her complaint." *Id*., n. 15.

No court has yet considered whether a patient list containing personally identifying information for patients of a specialized medical facility (such as an HIV clinic or infertility center) would constitute medical information under the CMIA. Post-*Eisenhower*, it remains to be seen how future courts will further interpret and clarify the requirements and application of the CMIA in this respect.

Don't forget HIPAA

It is noteworthy that *Eisenhower* does *not* address the question of whether the information contained in the index stored on the stolen computer qualified as "protected health information" under HIPAA. The CMIA's definition of "medical information" and HIPAA's definition of "protected health information" are similar, but expressed in somewhat different terms. Under HIPAA, "protected health information" subject to the HIPAA Security and Privacy Rules (45 C.F.R. Part 164, Subparts C and E) and the Breach Notification Rule (45 C.F.R. Part 164, Subpart D), includes individually identifiable information that "[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual" (45 C.F.R. § 160.103). Thus, the U.S. Department of Health & Human Services Office of Civil Rights has clarified that "an individual's health insurance card meets the statutory definition of PHI [protected health information]

and, as such, needs to be safeguarded." The *Eisenhower* Court concluded that, under the CMIA, information "regarding" an individual's medical history must "include" or "reveal" something about that history. The *Eisenhower* Court did not discuss whether, under HIPAA, information that "relates to" an individual's condition, treatment, or payment for health care must also include or reveal something about those matters.

In other words, after *Eisenhower*, the mere fact that an individual was a patient of a particular health care provider may not be "medical information" under the CMIA, but that information may still be "protected health information" under HIPAA. Those California covered entities and business associates subject to both HIPAA and CMIA should still extend the protections of the HIPAA Security and Privacy Rules to patient lists and similar information and, should they sustain a breach of an unsecured patient list or index, consider whether that event triggers their obligations under the HIPAA Breach Notification Rule. The *Eisenhower* case may offer some limits on civil liability, but should not be read to limit covered entities' and business associates' obligations to protect the privacy and security of protected health information, and to report data breaches, under HIPAA.

Stay Tuned: Another Significant CMIA Decision on the Horizon

Another significant case involving the scope of potential liability under the CMIA was recently argued before the California Court of Appeal. *Sutter Health et al. v. The Superior Court of Sacramento County*, No. C072591 (Cal. Ct. App. filed Nov. 29, 2012). This case involves the loss of patient data on a password-protected but unencrypted laptop computer. Sutter Health has argued, among other things, that because the plaintiffs failed to allege that medical information on the lost laptop was actually viewed by an unauthorized individual, the pleadings failed to state a claim for breach of the CMIA's confidentiality requirements. The Court of Appeal's decision may provide important additional clarification of the requirements for pleading and proof of claims under the CMIA.

Whatever happens in pending and future litigation relating to the CMIA, one thing remains certain: Parties with access to medical information should remain vigilant in their efforts to maintain such information privately and securely because patients and courts expect it and because the legal consequences of failing to do so, under the CMIA and HIPAA, and otherwise, can be substantial.

If you have any questions about the content of this alert, please contact the Pillsbury attorney with whom you regularly work, or the authors below.

Joseph R. Tiffany (bio)
Silicon Valley
+1.650.233.4644
joseph.tiffany@pillsburylaw.com

Connie J. Wolfe, Ph.D. (bio)
San Diego
+1.619.544.3139
connie.wolfe@pillsburylaw.com

Allen Briskin (bio)
San Francisco
+1.415.983.1134
allen.briskin@pillsburylaw.com