
No Harm, No Foul – Appellate Court Finds No CMIA Claim Without Actual Injury

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

California’s Confidentiality of Medical Information Act, Cal. Civ. Code § 56 et seq. (“CMIA”), provides that an individual may recover \$1,000 nominal damages (plus actual damages if any) based on the negligent release of medical information by a health care provider or other covered party. A California appellate court recently held that a health provider cannot be held liable for negligent release based on theft of medical records unless the plaintiff can establish that those records were actually viewed by an unauthorized person.

Following the trend of several recent data breach cases limiting the liability of health care providers, the California Court of Appeal, Third District, held last week that plaintiffs cannot make a CMIA claim when their medical records are stolen from their health care providers, unless those plaintiffs can allege that their information was actually viewed by an unauthorized person. *Sutter Health v. Superior Court (Atkins)*, No. C072591, 2014 WL 3589699 (Cal. Ct. App. July 21, 2014). In May 2014, the California Court of Appeal, Fourth District, held that plaintiffs could not establish a CMIA claim based on 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 2013, the California Court of Appeal for the Second District held that to obtain nominal damages for violation of the CMIA, a plaintiff must allege that “the confidential nature of the plaintiff’s medical information was breached as a result of the health care provider’s negligence.” *Regents of University of California v. Superior Court*, 220 Cal. App. 4th 549, 564-70 (2013). For further analysis of prior data breach cases, including a discussion of HIPAA implications and unresolved legal issues associated with data breaches, see our recent alert on [Eisenhower, California Court Limits Liability for Loss of Certain Patient Information under CMIA](#).

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.

Cal. Civ. Code § 56.101. Those 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).

In the recent *Sutter Health* case, some patients filed a class action lawsuit alleging CMIA claims based on the theft from a Sutter Health office of a computer containing their medical records, and claiming nominal damages for each class member (approximately \$4 billion). The *Sutter Health* court ruled that the plaintiffs did not have a claim under CMIA because they failed to allege that any unauthorized person actually viewed their medical records.

The *Sutter Health* holding was similar to *Regents*, but based on different grounds. The *Regents* court held that the theft of a computer containing medical records was sufficient to create a claim for violation of section 56.101 (negligent maintenance of records), but that a claim for \$1,000 nominal damages per person arising from the negligent “release” of medical information under section 56.36(b) could not be established without allegations that medical records were actually accessed, viewed or used by someone unauthorized to do so. The *Regents* decision also clarified that an actionable release would not require allegations of any affirmative communicative action on the part of a health care provider. *Regents*, 220 Cal. App. 4th at p. 560. In contrast, the *Sutter Health* ruling was based on the court’s determination that violation of section 56.101 could not be established by merely alleging that medical information came into the possession of an unauthorized person. Rather, the information must actually have been viewed by that person.

In *Sutter Health* 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. To violate the Act, “a provider of health care must make an unauthorized, unexcused disclosure of privileged medical information,” *Sutter Health* at *6, citing *Brown v. Mortensen*, 51 Cal. 4th 1052, 1070-71 (2011). 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. *Sutter Health* at *6. 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. *Id.* at *7. Applying this analysis to the allegations against Sutter Health, the court held that because plaintiffs had not alleged an actual breach of confidentiality, Sutter Health’s demurrer should have been sustained. *Id.* 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. *Id.*

Coupled with the *Eisenhower* and *Regents* decisions, the *Sutter Health* decision significantly limits the scope of potential liability for health care providers under the CMIA when their records are lost or stolen. California courts have now clarified that the theft of a patient list does not necessarily constitute a CMIA violation, because that list may not contain medical information, and that the theft or loss of medical information may not necessarily give rise to liability for damages unless it can be shown that the information was actually viewed by an unauthorized person. None of this, however, means that health care providers and others should let down their guard in connection with the privacy and security of medical information. Both the CMIA and HIPAA continue to apply, and require that health care providers and others continue to protect the privacy and security of medical and protected health information. The theft or loss of patient lists or medical information may still require reporting under HIPAA’s Data Breach Notification Rule (45 C.F.R. Part 164, Subpart C) and/or California’s electronic data breach notification rules (Cal. Civ. Code §§ 1798.29, 1798.82).

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

This publication is issued periodically to keep Pillsbury Winthrop Shaw Pittman LLP clients and other interested parties informed of current legal developments that may affect or otherwise be of interest to them. The comments contained herein do not constitute legal opinion and should not be regarded as a substitute for legal advice.

© 2014 Pillsbury Winthrop Shaw Pittman LLP. All Rights Reserved.