MORRISON FOERSTER

Calif. Case Limits Health Care Data Breach Claims

Law360
Andrew Serwin, Rebekah Kaufman, and Elizabeth Balassone

Appellate + Supreme Court, Class Actions, Privacy + Data Security

12/2/2013

Article

Law360, New York (December 02, 2013, 1:18 PM ET) -- The California Court of Appeal recently limited plaintiffs' ability to state a claim under the California Medical Information Act (CMIA), Cal. Civ. Code §§ 56 et seq., and their ability to get statutory damages under the act. Consistent with prior rulings in the data breach space, the court ruled that plaintiffs must plead and prove more than the mere allegation that a health care provider negligently maintained or lost possession of data, but rather that such data was in fact improperly viewed or otherwise accessed.

The Case

Plaintiff Melinda Platter brought a class action against the Regents of the University of California seeking damages from unlawful disclosure of confidential medical information in violation of the CMIA. Regents of the Univ. of Cal. v. Super. Ct., 220 Cal. App. 4th 549 (2013). She alleged that certain patients treated at UCLA health care facilities had personally identifiable medical information stored on an encrypted external hard drive that was stolen from a doctor's house in a home invasion robbery. Also missing was an index card near the computer that contained the password for the computer, which presumably would have permitted decryption of the data.

Plaintiff, on behalf of the class, alleged that the Regents had failed to exercise due care to prevent the unauthorized release or disclosure of confidential medical information. Plaintiff did not allege any actual damages, but sought $1,000 in statutory damages under CMIA Section 56.36(b) for herself and each putative class member. Section 56.36 provides that statutory damages of $1,000 are available for a patient whose confidential information was negligently released without proof that the plaintiff suffered or was threatened with actual damages.

The health care provider gave notice of the potential breach and informed potentially impacted patients of this incident. The letter stated that "[t]he theft was reported to the police and there is no evidence suggesting that your information has been accessed or misused."

The Regents demurred to the complaint, which was overruled by the trial court. On appeal, the Regents argued that Section 56.101 of the CMIA only allows a private right of action for negligent maintenance of confidential when such negligence results in unauthorized or wrongful access to the information.[1] This argument was based on the fact that there was no direct evidence that the information was improperly viewed or accessed. Plaintiff responded by arguing that the CMIA provides for statutory damages in any case where it can be proved that a health care provider's negligence was the proximate cause of an unauthorized third party obtaining protected information.

On Oct. 15, 2013, the court rejected plaintiff's argument and dismissed the action, finding that the CMIA requires pleading and proof that confidential information has been negligently released in violation of CMIA to bring a private cause of action for statutory and/or actual damages. Specifically, the court held, "[e]ven under the broad interpretation of 'release' we believe the Legislature intended in section 56.36, subdivision (b), as incorporated into section 56.101, 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. ... What is required is pleading, and ultimately proving, that the confidential nature of the plaintiff's medical information was breached as a result of the health care provider's negligence. Because Platter's complaint failed to include any such allegation, the Regents's demurrer should have been sustained without leave to amend and the case dismissed."

Focus on Legislative Intent

In its ruling, the court relied significantly on an analysis of the legislative intent behind Senate Bill No. 19 (1999-2000 Reg. Sess.), which added Sections 56.36(b)-(c) and 56.101 to the CMIA. The court cited to the Legislative Counsel's Digest of Senate Bill No. 19 to show that, by incorporating the entire 56.36(b) remedy into Section 56.101, the Legislature "plainly intended an action predicated on a health care provider's negligent maintenance of confidential information in violation of section 56.101 also plead and prove a release of that information."

The court also cited to the original language of Section 56.101 in Senate Bill No. 19, which stated, "Any provider of health care, health care service plan, or contractor who negligently disposes, abandons or destroys medical records shall be subject to the provisions of this part [the CMIA]." The court found this language to show, as originally enacted, that there was "no separate, stand-alone private cause of action for violation of section 56.101." Therefore, the incorporation of the Section 56.36(b) remedy "necessarily included the affirmative elements of the cause of action for negligent release of confidential information."

Benchmark for Health Care Data Breach Cases

The Regents case greatly limits a plaintiff's ability to state a claim for health care data breaches, absent proof that a plaintiff's information was specifically accessed, and not just lost. Under Section 56.101 of the CMIA, plaintiffs must plead and prove that their confidential medical information was actually viewed or otherwise accessed as a result of the health care provider's negligence. And in cases like Regents where the actual access is unknown, plaintiffs' claims fail because they cannot allege the information was, in fact, viewed by an unauthorized individual.

Reinforcement for Nonhealth-Care Data Breach Cases

The ruling also provides an interesting benchmark for data breach cases outside of the health care context that involve the loss of encrypted data and a password, because the court found that the potential loss of encrypted data, and the password, was insufficient to show that information was actually accessed by a third party. The Regents case reinforces prior decisions in nonhealth-care data breach cases that find that mere loss of data does not equate to an actual acquisition of data.

For example, in one case decided by the Third Circuit, the court rejected a claim under the Computer Fraud and Abuse Act alleging former employees repeatedly accessed plaintiffs' servers in order to obtain confidential information. P.C. Yonkers Inc. v. Celebrations the Party and Seasonal Superstore LLC, 428 F.3d 504 (3d Cir. 2005). The court found that plaintiffs had not shown they could prove their claims, because "[t]hat information was taken does not flow from mere access."

The issue was also addressed in a case alleging violation of the Fair Credit Reporting Act. Harrington v. ChoicePoint Inc., No. 2:05-cv-01294-MRP-JWJ (C.D. Cal. Oct. 11, 2006). Plaintiffs alleged that individuals had accessed certain computerized data possessed by ChoicePoint without authorization. Plaintiffs could not demonstrate that any information had actually been transmitted to the unauthorized individuals, and instead argued that in order to prove a "communication" that violated the FCRA, they need not demonstrate that any information was actually sent or received.

The court rejected this argument, finding plaintiffs' proposed meaning of communication was "at odds with the plain meaning of that word, which at minimum requires some act of transmission from one source or another." These cases, reinforced by Regents, support the view that potential access is insufficient to establish an acquisition of data under the security breach statutes.

Final Thoughts

Regents provides a benchmark for plaintiffs to plead and prove claims under the CMIA that is consistent with prior

nonhealth-care decisions: Plaintiffs must do more than plead mere loss of data. Practitioners should be on the lookout for further clarity and guidance as California courts begin to apply Regents.

—By Andrew B. Serwin, Rebekah Kaufman and Elizabeth Balassone, Morrison & Foerster LLP

Andrew Serwin is a partner in Morrison & Foerster's San Diego office. Rebekah Kaufman is a partner and Elizabeth Balassone is an associate in the firm's San Francisco office.

[1] Section 56.101 provides in part that "[a]ny provider of health care, health care service plan, pharmaceutical company, or contractor who negligently creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information shall be subject to the remedies and penalties provided under subdivisions (b) and (c) of Section 56.36."