Despite data privacy law, victims see damages hurdles

Plaintiffs struggle to plead cases successfully even after a security breach takes place

By Omar Shamout
Daily Journal Staff Writer

Kaiser Permanente this month notified 49,000 of its patients that a flash drive containing their personal medical records disappeared from a secure area at Anaheim Medical Center. Such data privacy breaches have become more frequent as medical records are increasingly digitized, but health care providers may be relieved to know that the threat of liability in such incidents is still somewhat contained.

Though regulatory experts say California has one of the oldest and best established health privacy laws in the country, a recent class action case that tested the limits of when consumers can claim statutory awards for medical privacy violations did not end well for plaintiffs.

Lawyers have looked toward claiming statutory damages in state courts to avoid the obstacle of proving out-of-pocket damages in federal class actions. The state's Confidentiality of Medical Information Act entitles individuals to a nominal $1,000 award if health care providers disclose their medical information without authorization — an amount that jumps sharply when multiplied by the thousands of members of a potential class. Another law protects consumer financial data, and a different statute requires notification of individuals in the event of a breach involving certain types of information, such as social security, driver's license, payment card and bank account numbers.

But even statutory damage class actions have to clear significant hurdles, as Los Angeles attorney Brian S. Kabateck of Kabateck Brown & Kellner LLP found out two months ago when a suit he filed in Los Angeles County Superior Court against the Regents of the University of California was dismissed on appeal without leave to amend.

A lower court had overruled the regents' demurrer to the complaint, but the 2nd District Court of Appeal vacated the order on the grounds that the plaintiff couldn't prove her information was "improperly viewed or otherwise accessed."

The case concerned the personally identifiable medical and financial information of 16,000 UCLA Health System patients stored on an external hard drive. A UCLA physician took the hard drive to his house in Honolulu in September 2011, where it, along with the password for the encrypted information, was stolen during a home-invasion robbery.

Justices Dennis M. Perluss, Fred Woods and Laurie D. Zelon unanimously ruled the plaintiffs' pleading failed to meet the requirements of an actionable claim under the Confidentiality of Medical Information Act.

"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," the panel said. *The Regents of the University of California v. The Superior Court of Los Angeles County*, 2013 DJDAR 15066 (Oct. 15, 2013).

Given the thief isn't in custody and available to testify, a civil procedure expert said that's a hard thing to prove. "It's almost like there's no way to plead it any differently," said Georgene Vairo, a professor at Loyola Law School.

Kabateck and co-counsel Richard N. Kellner filed a petition for rehearing and asked the court to grant them leave to amend based on supposed new evidence that an unauthorized telephone account was opened in the plaintiff's name "within months" of the robbery. Justices ruled it was too little too late.

"[Plaintiff] had not alleged that any person accessed, viewed or used the confidential information on the external hard drive," they said. "There are simply too many layers of speculation required for these minimal facts to be considered sufficient to overcome the deficiency in [the plaintiff's] complaint."

Kabateck said he was frustrated the court did not give him the opportunity to try to make his case that someone must have looked at the information based on the evidence. "It doesn't have to be disseminated to the world," he said. "At the very least the bad guy would have looked at the information."

Vairo added the plaintiffs also had a right to be upset since the appeals court took the decision to re-plead away from the trial judge.

"That's kind of harsh," she said, adding that the ruling amounted to the justices telling the plaintiffs "we're creating new rules, but we're not going to let you play by those rules."

Defense attorney Bradley S. Phillips of Munger, Tolles & Olson LLP in Los Angeles, who represented the university, said it was obvious from the opinion that the justices thought any future pleadings would be "futile" based on their interpretation of the statute.

The decision in the UC Regents case could also have a big effect on a similar matter before the state's 3rd District Court of Appeal in which a class of more than 4 million plaintiffs is seeking $4.2 billion from Sacramento-based insurance provider Sutter Health for unencrypted information compromised when a computer was stolen from Sutter's offices. *Sutter Health et al. v. The Superior Court of Sacramento County*, C072591 (Cal. App. 3rd Dist., filed Nov. 29, 2012).

The health care company's attorney, Robert H. Bunzel of Bartko, Zankel, Bunzel & Miller PLC in San Francisco, notified the 3rd District of the 2nd District opinion immediately.

Plaintiffs' attorney, Michael Ram of Ram, Olson, Cereghino & Kopczynski in San Francisco, had earlier contended that the law's language "plainly focuses on the actions of the person or entity that failed to keep medical information confined, and not on events that may transpire after that release, such as viewing or review" by a third party.

In an interview with the Daily Journal, Ram said the previous appellate ruling "seemed inconsistent" with the spirit of the statute, adding that the state Supreme Court might ultimately need to weigh in on the issue.

"That's why the Legislature created these remedies without the need to prove actual damages," Ram added, though he said he remains hopeful the justices reviewing his case might still come to a different conclusion than their 2nd District colleagues. Oral arguments are expected in early 2014, though no date has been set.

Bunzel declined to comment on the pending litigation, but Phillips said he didn't see how the Sutter class action could continue in light of the appellate ruling in his case.

"It should dispose of that case," Phillips explained. "I don't believe there's evidence anyone saw the information."

Despite his court defeat, Kabateck, who recently finished a yearlong stint as president of the Consumer Attorneys of California, the state's tort lawyer lobby, said he expects more data regulation down the road. Legislators could be inclined to enact legislation protecting even more types of information in an effort to assuage public fears that online identities are increasingly vulnerable to lax security and prying eyes.

KABATECK

That means additional lawsuits, Kabateck added, especially since attorney fees are recoverable in injunctive relief cases stemming from gaps in security, even when no damages are sought.

"More privacy statutes are going to be drafted and modeled on the medical privacy statute," Kabateck said. "It gives a blueprint for future legislation."

Privacy expert Lisa J. Sotto of Hunton & Williams LLP said in an email that she's confident more laws will be passed on both the state and federal level to further protect children's information, geolocation data, and health and financial records. "No question about it."

omar_shamout@dailyjournal.com