Court to Decide if a Stolen Hard Drive Is Worth $4 Billion

Scott Graham

2013-01-25 02:34:24 PM

Whoever threw a rock through a window and broke into Sutter Medical Foundation's administrative offices the weekend of Oct. 15, 2011, probably didn't realize the computer they were stealing could be worth $4 billion.

The PC contained a hard drive with confidential information for 4 million patients, and California's Confidentiality of Medical Information Act provides nominal damages of $1,000 per individual for negligently released data.

Within a month, 14 law firms had brought 13 complaints against Sutter, with the cases now consolidated in Sacramento County Superior Court. But to date, there's been no clear indication that the data from the stolen computer — which was password-protected but not encrypted — has been misused or even viewed by a third party.

Now the Third District Court of Appeal has intervened, staying proceedings Jan. 17 and ordering briefing on whether the theft of the computer alone amounted to a release of confidential information. "'Confidentiality' is lost only when the information becomes known to someone else — when it is no longer secret, concealed, private, unrevealed or undisclosed," Bartko, Zankel, Tarrant & Miller partner Robert Bunzel argued in Sutter's petition for writ of mandate.

The stakes are enormous not only for Sutter, but for California's entire health care industry. Hospitals and health care providers are litigating at least nine similar class actions around the state. They "face similar staggering exposure, even in the absence of any evidence that their patients have suffered any actual injury through alleged invasion of their privacy interest," wrote Crowell & Moring partner Ethan Schulman on behalf of *amicus curiae* California Association of Health Plans and the Association of California Life and Health Insurance Companies.

But actual injury has in fact occurred, say the attorneys representing the Sutter patients. "Once you know a computer containing your personal medical data is stolen, your peace of mind is gone," says C. Brooks Cutter of Sacramento's Kershaw, Cutter & Ratinoff. And when stolen data is used to commit identity theft crimes, it's not always obvious where the data came from, he adds.

That's why the statute imposes liability for mere "release" of information, and does not explicitly require disclosure to a third party, Cutter and his co-counsel contend.

Sacramento Superior Court Judge David De Alba agreed with the plaintiffs. "The term 'released' is not uncertain, ambiguous or doubtful" in the context of the confidentiality act, he wrote in his Oct. 11, 2012, ruling now under review by the appellate court. "The term does not include the concepts of review or use by the person or entity to whom the information is released."

EASY TO ENCRYPT

Discovery is not yet under way, but Sutter admits that data for 4.2 million patients was stored on the hard drive of the desktop computer. For 943,000 patients of Sutter Medical Foundation, the data included information about their medical conditions. For 3.3 million patients of affiliated providers, data was limited to name, address, phone, email, date of birth, medical record number and insurance provider, Sutter says.

Sutter says it doubts the thief or thieves were targeting the data, because a keyboard and monitor were stolen as well. Nor has the data turned up on Internet hacker sites. "There is no allegation that a single word of the password-protected information on the hard drives in the stolen computer has been read by any unauthorized person," Bunzel wrote in his petition.

Sutter waited a month to report the data breach to patients, notifying them Nov. 16, 2011. The first lawsuit was filed the same day, the company says. Kershaw Cutter, Sacramento's Dreyer Babich Buccola Wood Campora and San Francisco's Ram, Olson, Cereghino & Kopczynski have been designated lead counsel.

Plaintiffs counsel say there's no doubt Sutter negligently stored or maintained confidential medical information, as prohibited by the Confidentiality of Medical Information Act, California Civil Code §56. The data were not encrypted, and the company didn't so much as set up an alarm system to alert against intruders. "It's clearly the industry standard, to have data encrypted," Cutter says, and it's not expensive to do.

Sutter Medical Information Cases, JCCP 4698, is already on its third trial judge. The case was originally assigned to Sacramento County Judge David Abbott, but when Sutter determined he was one of the patients whose data was on the hard drive, he recused himself. One of the plaintiffs firms filed a peremptory challenge against the next judge assigned, Raymond Cadei, and the case was assigned to De Alba.

'NOT ABSTRACTIONS'

Sutter raised numerous issues in its petition to the court of appeal, but the court asked it to focus on one: whether actual disclosure of data to a third party is necessary to state a claim. "The unmistakable goal of the requirements about 'disclosure' and 'release' is the protection of an individual from the invasion of his or her privacy," Bunzel wrote in his petition. "These are not abstractions."

Bunzel points to a 1996 California Supreme Court ruling, *Heller v. Norcal Mutual Insurance*, 8 Cal.4th 30, which holds that to violate the confidentiality act, "a provider of health care must make an unauthorized, unexcused disclosure of privileged medical information." In this case, there's no unauthorized viewing, Bunzel wrote. Federal courts have similarly construed U.S. privacy laws, he contends.

In his *amicus* letter. Crowell & Moring's Schulman says the Legislature that first enacted the confidentiality law in 1979 could not have foreseen electronic storage of medical records. "At the same time, rapid advances in computer storage and communication technologies, including mobile and wireless Internet communication, have dramatically increased the challenge of maintaining the security of such information," wrote Schulman, whose client, Health Net of California, is facing class actions in three state and federal courts over missing server drives.

The plaintiffs say the case isn't that complicated. Civil Code §56.36(b) explicitly prohibits negligent "release" of information — a term they say is broader than "disclosure." And §56.36(b)(1) — the part providing for $1,000 nominal damages — specifies that "it shall not be necessary that the plaintiff suffered or was threatened with actual damages."

"We believe the statute as well as the legislative history are very clear on this," said Tina Wolfson of Los Angeles' Ahdoot & Wolfson, who co-wrote the plaintiffs appellate opposition.

The federal statutes and court decisions aren't relevant to the California statutory scheme, they argue, and mobile and wireless technology is completely beside the point. "The nature of the breach doesn't arise from sharing," Cutter says. "It arises from their basic duty to secure the data in their own headquarters building."