


# THE RECORDER

 [Click to Print](#) or Select 'Print' in your browser menu to print this document.

Page printed from: [The Recorder](#)

---

## Justices Skeptical in Health Care Data Breach Case

Cheryl Miller, The Recorder

June 20, 2014

SACRAMENTO – Plaintiffs seeking damages from a health care network that lost information about 4.2 million patients in a computer theft faced tough questioning during oral arguments Friday from a Sacramento appellate court.

The Third District Court of Appeal panel, led by Justice George Nicholson, quizzed plaintiffs' counsel about claims that Sutter Medical Foundation patients' confidentiality was breached, even though there's no evidence the patient data was ever viewed or misused after the 2011 theft. Sutter is challenging a 2012 trial court ruling that the negligent "release" of information alone triggered liability and did not require disclosure to a third party.

Nicholson and Justice Louis Mauro continually probed whether California's Confidentiality of Medical Information Act, implicitly or otherwise, requires proof that the released data was viewed.

"Where in your pleading do you assert there's been a breach of confidentiality?" Nicholson asked.

"We contend the breach of confidentiality occurred the moment the computer walked out of Sutter," C. Brooks Cutter of Kershaw, Cutter & Ratinoff responded.

"There was a password" on the computer, Nicholson added.

"Which is easily hacked," Cutter said.

The case is being closely watched by California's health care industry, which is facing at least nine class actions tied to claims that hospitals and medical groups disclosed patient data in violation of state statute. The medical confidentiality statute provides damages of \$1,000 per individual for negligently released data. If found negligent, Sutter could theoretically face damages of \$4 billion.

The Sutter data was put at risk when someone broke into the company's administrative headquarters in October 2011 and stole a computer with password-protected but unencrypted patient data. Within a month, 14 law firms had filed 13 complaints against Sutter. Those cases were consolidated in Sacramento County Superior Court.

Sutter attorney Robert Bunzel of Bartko, Zankel, Bunzel & Miller argued Friday that plaintiffs are trying "to create a private right of action that the Legislature did not intend to create." No injury exists until a patient's privacy is violated, he said.

"This case is about privacy. The history and purpose of the [confidentiality] statute is all about privacy," Bunzel said.

But plaintiffs have argued that they suffered actual injury simply in the loss of peace of mind. And when identity theft crimes occur, it's not always obvious where the stolen data came from, counsel have argued.

For 943,000 Sutter Medical Foundation patients, the stolen data included information about their medical conditions. For the remaining 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 said.

*Senior Writer Scott Graham contributed to this report.*

Contact the reporter at [cmiller@alm.com](mailto:cmiller@alm.com).

