California Courts Decide When a Data Breach is not a Data Breach

October 31, 2014 - California is a funny place. The state has some of the toughest privacy laws of any state; laws which extend to medical records. Not only are the state's laws tough, California is often on the forefront with new legislation that addresses new threats to privacy. For instance, the state that enacted the first data breach notification law was California. So it is somewhat ironic that these tough laws enacted by the state legislature are being weakened by the state's court system.

At the end of 2011, we told you about a data breach at Sutter Medical Foundation that involved more than 4 million people. A law suit followed that was brought under a state law; the Confidentiality of Medical Information Act. The law states that a health care provider "who negligently creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information shall be subject to the remedies and penalties." The law goes on to specify that penalty for such a breach is up to $1,000 per patient. In this case, that would amount to more than $4 billion.

Sutter argued that there was no way to know if the data contained on the computer had been used for fraudulent purposes or if it was ever accessed by whoever stole the computer. They went on to say that there was no way for the plaintiffs in the case to prove that the stolen data had ever been accessed or that anyone could attribute a single case of identity theft or fraud to the breach.

Sutter lost their argument in court but the company appealed the decision. The appellate court overturned the lower court's ruling. And this week, the California State Supreme Court refused to hear another appeal in the case. That means that the appellate court ruling will stand.

The ruling means that unless residents of California can prove that a specific medical data breach has resulted in some form of financial fraud against them, they have no right to sue the breaching party or to pursue damages.

The ruling sets a dangerous precedent in a state that has been on the leading edge of privacy rights. Even though the victims of this breach are going to have to monitor their health and financial records for the rest of their lives, they have no recourse against the company that breached their data. Furthermore, with this standard it will be very difficult for anyone to prove that they have been victimized by a specific data breach going forward. This means that companies have little or no incentive to invest in systems to protect the consumer data that they store and it eviscerates the law.

ACCESS urges the California State Legislature to take up this issue soon and to restore enforcement of the consumer's right to the privacy of their medical records.
byJim Malmberg
Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.
Follow me on Twitter:

Follow ACCESS