A $4 Billion Dollar Health Breach? Practical Suggestion to Avoiding CMIA Liability and Other Lessons of Sutter Health v. Superior Court

If you ask most California healthcare providers about the risks associated

health information data breaches, chances are they will mention HIPAA. More knowledgeable providers may even be aware o serious risks for failing to respond appropriately to data breaches. Ask the same providers about the risks they face under California's Confidentiality of Medical Information Act (CMIA), and the likeliest reaction is blank stares.

The irony is that the more practical and immediate risk for many providers arise under the CMIA, rather than HIPAA. That's because, while HIPAA is enforced by the government, principally through investigations and fines, any private party can bring lawsuit for monetary damages for violations of the CMIA. The statutory damages of $1,000 per person under the CMIA may n sound like much, but more and more class action lawyers are interested in suing when a data breach involves information rela to groups of patients.

As more data breach cases hit the California courts, California courts have been forced to wrestle with the tension between th legislative mandate to secure health data and not creating an excessive burden on healthcare providers when data breaches occur. Two recent cases reflect the way that the judicial understanding of provider responsibilities and liabilities for data breac are evolving.

In *Regents of the University of California v. Superior Court*, 220 Cal. App. 4th 549 (2013) a physician's laptop containing thou of patient health records was stolen. The Court concluded that a 'disclosure' by the defendant provider was a necessary elem private party damages under the California Medical Information Act, Cal. Civ Code Sec. 56 et seq. (CMIA). Based on the abse of any allegations regarding what had happened to the data after the computer was stolen, the panel found no *affirmative* disclosure by the defendant. While ruling for the defendant in requiring its affirmative act before a wrongful disclosure was fou dicta the *Regents* court rejected the notions that actual viewing of the records or some proof of harm to the plaintiffs were req elements of private party damages.

Last month, a different appellate panel disagreed as to what was required for CMIA private party damages, concluding that pr the traditional elements of the tort of negligence were needed to meet the statutory requirements for a private party damages award. In Sutter Health v. Superior Court, ___Cal. App. 4th ___ (No. C072591, Third Dist. July 21, 2014) a computer containi over 4 million health records was stolen from a Sutter Health medical records facility. Plaintiffs brought suit seeking, on behalf themselves and a class of similarly situated patients, the CMIA statutory damages of $1,000 per breach. The records were password protected, but the patients' attorney argued that the CMIA provided for strict liability for any breach based on Sutter admission that the records fell into the hands of an unauthorized party. The trial court denied Sutter's demurrer. Sutter filed a mandate challenging the lower court decision, and the appellate court reversed on the basis that plaintiffs had not alleged tha unauthorized person had actually viewed the records. The appellate court concluded that a private party may only be awarded damages upon proof of (1) a breach by defendant of a (2) statutory duty owed to plaintiff, (3) resulting in injury to plaintiff, (4) caused by the defendant's breach. In short, absent proof that there was actual viewing of the health records by an unauthoriz person, there was no cause of action properly stated.

Healthcare providers may take comfort in the Sutter Health court's attempt to impose a limit of reasonableness before allowin

the risk of a $4 billion liability. At the same time, providers should not rest too easy: there is not a clear legislative record that t negligence/tort framework should be applied to the CMIA and the argument for strict liability is almost certain to resurface. As result, it is not yet clear whether the holding of Sutter will become generally accepted. And despite the unexceptional tort law holding in Sutter, there remain numerous unanswered questions.

What, for instance, are the minimum steps a provider in possession of health care data must take to meet its duty to protect patients' data from inadvertent disclosure? Or despite all the encryption and security efforts, is a mere disclosure and mere vi of data sufficient to meet the elements of a violation? Does the unauthorized party need to actually know what he or she is loo at, e.g., would proof that the data burglar had no medical or other training to be able to discern what the health information me mean that there was no disclosure? Can hospitals, physicians and insurance companies rely on state-of-the-art IT programs a expert IT advice as to what steps are appropriate to try to prevent phishing and hacking of data, or is someone's mere breach IT firewall into a data pool sufficient to state a cause of action?

The Sutter Health ruling highlights that healthcare providers should not limit their focus to HIPAA compliance, but must be als attuned to evolving state law. Despite the seemingly favorable nature of the ruling for hospitals, physicians, and their insuranc companies, there remain big questions ahead about the limits of the duty to prevent health information disclosures. As a pract matter, we recommend to many healthcare provider clients that they consider the HITRUST Common Security Framework (C ensure that their health data compliance strategies are consistent with best practices for organizations of their type and size.