OBER | KALER
Attorneys at Law

October 11, 2011

Ober|Kaler Healthcare Information Privacy, Security and Technology Bulletin

James B. Wieland | jbwieland@ober.com

Joshua J. Freemire | jjfreemire@ober.com

Data Breach in California Results in $20 Million Class Action

The new Director of the HHS Office of Civil Rights ("OCR") has promised to continue the agency's trend towards greater HIPAA enforcement, but, following a data breach, OCR may not be a provider's or contractor's only concern. On September 28, Shana Springer, a California woman whose protected health information was unknowingly made public, along with the information of approximately 20,000 other emergency room patients, filed a class action lawsuit in Los Angeles County Superior Court. The suit seeks approximately $20 million in damages from the hospital ultimately responsible for the breach, Stanford Hospital & Clinics.

The suit follows a breach that was originally made public in early September. A spreadsheet containing data (including patient names, diagnosis codes, dates of treatment, and billing information) on 20,000 patients treated in the Stanford emergency department during a six month period in 2009 was discovered as a publicly available document on the website Student of Fortune. Student of Fortune is a public site designed to allow students to seek paid help with their homework by posting assignments. The information had originally been entrusted to a Los Angeles billing contractor, Multi-Specialty Collection Services. Neither Student of Fortune nor Multi-Specialty Collection Services has explained how the spreadsheet came to be posted to the publicly available Student of Fortune database. When the information was discovered by a patient and Stanford

notified, the spreadsheet was immediately removed from the Student of Fortune website and the data breach was reported to HHS OCR.

Most providers and contractors are aware that HIPAA does not provide for a private right of action. HIPAA, however, does not preclude actions under state laws.[1] HIPAA, however, is only part of the puzzle when it comes to privacy or security breaches. Most states have now passed one or more statutes (California currently has several) that also require that entities keep client and patient personal and financial data secure. These laws are not necessarily limited to covered entities and business associates as defined by HIPAA, although the laws tend to focus on either medical information or personal information such as social security numbers. State laws can reach to any entity that is an owner or licensee of protected personal information or that otherwise maintains such information. Since HIPAA does not preempt state laws which provide individuals with greater privacy rights or protections, state laws that reach beyond HIPAA, or provide additional rights or remedies, are not preempted.

Ms. Springer's suit relies on just such a state law, the California Confidentiality of Medical Information Act ("CMIA"). The CMIA not only provides for a private right of action, it specifically provides that patients whose data is disclosed unlawfully may bring suit to recover nominal damages ($1,000) even where they neither suffered nor were threatened with actual damages. In other words, though Stanford has vowed to fight the suit, California's state law in general provides a very low bar to plaintiff's seeking the type of redress sought by Ms. Springer.

Twenty-thousand individuals may sound like a lot, but, in the world of breaches of electronic data, it is not a surprising number. A similar breach, discovered in August, led to the disclosure of 300,000 patients' information. At $1,000 per patient, that could involve potential liability of $300 million dollars. Even for large providers, "nominal" damages in such a scenario could quickly become a matter of "bet the company" litigation.

An ounce of prevention, when it comes to breaches, is worth a pound of cure. Providers who outsource data, especially large volumes of electronic data, should take the Stanford case as a warning of things to come. Even if Stanford successfully defends the litigation, the costs of a defense (both financial and reputational) can be extremely high. There is no magic bullet to defend prevent a breach, but good security protections, particularly encryption, vigorous employee training and monitoring, and careful selection of contractors who receive protected personal information can go a long way.

---

1 The HITECH Act also gives state attorneys general the right to bring a civil action for HIPAA violations on behalf of citizens of the state, although damages are capped by the statute.

It goes without saying that providers and contractors should be aware of both the federal HIPAA rules and any applicable state laws that might, as California's, reach beyond the protections of the HIPAA Privacy and Security rules. Covered entities should ensure their privacy policies and procedures are thoughtfully drafted and vigorously enforced, but they must also review the capabilities and practices of their contractors and ensure that business associates contracted to handle data are subject to strict supervision. From the contractor's perspective, the ability to offer appropriate privacy and security protection for customers' data may become a condition of doing business, especially where the business involves medical or other personal information. Both providers and contractors should also pay close attention to any applicable contractual indemnification provisions and each party's information practices insurance. In the light of the Stanford case, contractual negotiations regarding these points is likely to take on a new urgency.

About Ober|Kaler

Ober|Kaler is a national law firm that provides integrated regulatory, transaction and litigation services to financial, health care, construction and other business organizations. The firm has more than 130 attorneys in offices in Baltimore, MD, Washington, DC and Falls Church, VA. For more information, visit www.ober.com.
