OBER | KALER
Attorneys at Law

Health Law Alert™

Subscribe | Health Law Group | Health Law Alert Archive

2011 Issue 4

www.ober.com

UCLA Resolves Privacy and Security Rule Violations

By: James B. Wieland and Joshua J. Freemire

Curious employees are getting expensive. In a July 6, 2011 Resolution Agreement and Corrective Action Plan (CAP) [PDF], the Regents of the University of California, on behalf of the University of California at Los Angeles Health System, agreed to pay $865,500 and enter a three-year compliance monitoring and reporting program (a "corrective action plan" or CAP) for a HIPAA violation. While several violations are described in the settlement documents, the main issue will likely be familiar to many hospital and health system privacy officers: curious hospital employees regularly perused patient medical records which they had no valid reason to access.

While the settlement documents don't specify, it is a reasonably good guess that the UCLA patients in question are (or were) celebrities. The temptation, for many employees, to get a sneak peak at some unfiltered celebrity gossip has a well-documented negative influence on compliance. It is worth noting, however, that the settlement documents specifically do not mention why the patient records were accessed — in point of fact, it simply doesn't matter. A facility may not be surrounded by paparazzi, but the temptation for employees to access medical records of friends, family, neighbors, and well-known local personalities can be just as high. The risk of "curious employees" then, is by no means limited to hospitals within sight of the Hollywood sign. All covered entities should take a lesson from the UCLA settlement.

The Resolution Agreement notes that an HHS OCR investigation was initiated in June 2009 following two complaints regarding inappropriate access to patient medical records. Following the investigation, HHS OCR identified five compliance failures:

- During two and a half months in 2005 and three days in 2008, UCLA workforce members "repeatedly and without a permissible reason" accessed and examined the protected health information of specific UCLA patients;
- From 2005 through 2008, an employee in the office of UCLA's Director of Nursing office "repeatedly and without a permissible reason" accessed and examined the protected health information of "many patients";
- From 2005 through 2008, UCLA failed to provide (or failed to document the provision of) appropriate Privacy and Security Rule training for all members of its workforce;
- From 2005 through 2008, UCLA failed to appropriately sanction workforce members who inappropriately accessed records; and
- From 2005 through 2008, UCLA failed to implement "security measures sufficient to reduce the risks of impermissible access to protected health information by unauthorized users to a reasonable and appropriate level."

UCLA settled these allegations without admitting any wrongdoing, by agreeing to pay a settlement of $865,500 and to enter into a three-year compliance monitoring agreement (the CAP).

The general form and content of CAPs, and the burdens they can impose, are addressed separately in "Corrective Action Plans Can Mean Significant Compliance Monitoring Requirements for Covered Entities that Settle HIPAA Complaints." In addition to the typical requirements of updated policies and procedures (which must be approved by HHS), workforce retraining, and regular reporting (annually and in the case of any "reportable events" such as further security breaches), the UCLA CAP also requires that UCLA designate and retain an independent monitor at its own expense. Under the CAP, the Monitor is tasked with conducting regular surprise site visits, interviewing employees, reviewing UCLA's compliance and internal monitoring plans, and preparing its own annual report for HHS. The nearly million dollar fine, in other words, is only the tip of the iceberg in terms of the administrative costs and burdens the settlement imposes on UCLA.

The settlement also raises at least one important and unanswered question: What is a “reasonable and appropriate” level of risk when it comes to risk of unauthorized workforce access to patient medical records? It is certainly simple enough, if the patient in question is a famous celebrity, to lock-down access to his or her records, but how should facilities react when a local TV reporter arrives for treatment? A state legislator? A popular but reclusive novelist? A patient who is well known by hospital staff? It would certainly seem unreasonably burdensome and impractical to require that each hospital member obtain separate privacy officer authorization for each record that they access. But it seems equally impractical to require that each facility make its own independent judgment with regard to who is famous enough, important enough, or wealthy enough to warrant special treatment. The “reasonable” standard, in this case, leaves facilities in a difficult position.

Ober|Kaler's Comments

Human engineering has its limits. It is not always possible for facilities to entirely prevent workforce members from viewing records that they shouldn’t. It is possible, however, for facilities to ensure their workforce members are well educated with regard to facility policies, including the policies governing sanctions. It is also possible for facilities to act, swiftly and decisively, to sanction workforce members who have violated facility policies. It may seem harsh, but robust, clear policies, a well-documented training program, and a history of sanctioning non-compliant workforce members may prove to make a difference in the bargaining position of a health care facility in an HHS OCR investigation or audit.