AKIN GUMP
STRAUSS HAUER & FELD LLP

Privacy and Data Protection Alert

UCLA Health System Settles Potential HIPAA Violations as HHS Awards Contracts to Implement the HIPAA Audit Program

July 12, 2011

On July 7, 2011, the U.S. Department of Health and Human Services (HHS), Office for Civil Rights (OCR) announced a resolution agreement with the University of California at Los Angeles Health System (UCLAHS) for potential violations of the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules. UCLAHS agreed to pay $865,500 and enter into a three-year corrective action plan (CAP) to resolve the OCR investigation. This agreement is the latest in a string of HIPAA enforcement actions announced by OCR—including the first-ever civil monetary penalty totaling over $4.3 million imposed against Cignet in February 2011—and comes as OCR makes significant progress in rolling out the HIPAA audit program mandated by the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009. In June 2011, HHS awarded contracts to KPMG and Booz Allen Hamilton to assist OCR in operating the audit program.

The resolution agreement involves two separate complaints concerning celebrity patients, alleging that unauthorized UCLAHS employees repeatedly accessed the patients' electronic protected health information (PHI). The complaints stated that UCLAHS failed to appropriately train employees to ensure sufficient privacy protections and also failed to sanction and/or document sanctions of employees who impermissibly examined the patients' PHI. The complaints were likely not the only tip that set off the OCR investigation. In April of 2008, UCLAHS's chief compliance and privacy officer confirmed to the *Los Angeles Times* that the health system had detected that unauthorized employees were inappropriately viewing patient files, including those of Farrah Fawcett.

The CAP requires UCLAHS to review and revise its policies and procedures regarding permissible uses and disclosures of PHI—which HHS must approve —and to implement appropriate sanctions for any violations. UCLAHS must provide training on the policies and procedures to all workforce members who have access to PHI. The CAP also requires UCLAHS to report any violation of its policies and procedures—which may or may not constitute violations of HIPAA regulations—within thirty days of determining that a violation exists. An independent monitor will be designated to investigate, assess, and make specific determinations about UCLAHS' compliance with the requirements of the CAP. The monitor will, among other duties, conduct at least two unannounced site visits per year to determine whether workforce members are complying with UCLAHS' policies and procedures, and will generate various reports.

Future OCR enforcement actions seem even more likely as HHS recently announced plans to implement the HITECH-mandated HIPAA audit program. In June 2010, HHS awarded contracts to Booz Allen Hamilton for $180,000 to develop methods to identify audit candidates and to KPMG for $9.2 million to develop an audit protocol and conduct audits of HIPAA covered entities and business associates. HHS expects that each audit would include a site visit during which auditors would interview the entity's leadership (e.g., the chief information officer, privacy officer, legal counsel, health information management/medical records director); examine the physical features and operations of the entity; observe whether the entity's processes track its policies; and review the entity's compliance with HIPAA regulatory requirements. HHS will require KPMG to submit a detailed written report of each audit, which must include specific recommendations for actions that the audited entity can take to address identified compliance violations through a CAP. Importantly, HHS will require KPMG to demonstrate clearly that each of its negative findings is a potential violation of

the HIPAA Privacy or Security Rule. The audit program may be implemented quickly; up to 150 audits may be completed by the end of 2012. The audits represent an important HITECH-driven departure from past OCR practices, which historically relied upon complaints before conducting investigations.

HIPAA covered entities and business associates should take prompt action to prepare for potential audits and investigations. Now is the time to confirm that all appropriate HIPAA compliance documentation is in place and current, to ensure that all workforce members who have access to PHI have received adequate training, and to engage in a thoughtful review of privacy and data security policies and procedures.

CONTACT INFORMATION

If you have any questions concerning this alert, please contact—

Jo-Ellyn Sakowitz Klein
jsklein@akingump.com
202.887.4220
Washington, D.C.

Anna R. Dolinsky
adolinsky@akingump.com
202.887.4504
Washington, D.C.

Kristen Henderson
khenderson@akingump.com
202.887.4587
Washington, D.C.