Issue 2, Summer 2012

This newsletter is prepared by the Office of Compliance and is intended to provide you with current information about healthcare compliance and HIPAA privacy issues. For additional information, to view past newsletters, or to provide comments about this or any future issues of this newsletter, please contact the Office of Compliance at (213) 740-8258 or at complian@usc.edu.

HIPAA Audit Program Protocols Released

On June 26, 2012, the Department of Health and Human Services ("HHS") Office for Civil Rights ("OCR") posted on its website the protocol it developed to serve as a guideline for the recently-implemented Health Insurance Portability and Accountability Act of 1996 ("HIPAA") compliance audits. Mandated by the Health Information Technology for Economic and Clinical Health ("HITECH") Act, which was enacted as part of the American Recovery and Reinvestment Act of 2009, these audits are conducted as part of the new OCR HIPAA Audit program (the "Audit program") which is intended to assess covered entities' compliance with the HIPAA Privacy, Security, and Breach Notification Rules. Similarly to how the USC Office of Compliance assess and monitor compliance with these requirements, the audits examine:

- How the organization (covered entity) manages the process of providing the notice of privacy practices for protected health information (PHI), limits access of individuals to PHI, examines the appropriateness of uses and disclosures of PHI, abides by patient rights with respect to requests for amendments of PHI and tracks accounting of disclosures in addressing the Privacy Rule requirements;
- Whether the organization includes risk assessments, develops and employs an information system activity review process, and evaluates existing security measures related to access controls to address the Security Rule requirements for administrative, physical and technical safeguards;
- How the organization provides risk assessment when determining if a potential breach exists and ensuring that breach notification to individuals in a timely manner are provided in a timely manner to address the Breach Notification Rules.

While OCR officials have stated that the audits are intended to serve as a "compliance improvement tool," they have also been clear that enforcement actions may be taken if OCR finds a lack of compliance or cooperation with the audit. At the same time, OCR has continued to increase its enforcement activity and publicized many recent settlements and penalties which highlight the high-risk nature of this area of compliance.

More information about the HHS HIPAA audit pilot program is available at: http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/index.html

Laptop Data Breaches Underscore the Importance of Encryption on Laptops and Mobile Storage Devices

The University of Texas MD Anderson Cancer Center is notifying

30,000 patients of a data breach after an unencrypted laptop was stolen from a faculty member's home. The data included patients' names, medical record numbers, treatment and/or research information, and in some instances social security number, and was on an unencrypted computer stolen from an M.D. Anderson faculty member's home.

This breach comes on the heels of a breach reported in May, when an employee of Boston Children's Hospital who was attending a conference in Buenos Aires lost a laptop containing unencrypted health information of more than 2,100 patients. Last year, UCLA reported that medical information for 16,288 patients may have been compromised when a faculty member's home was burglarized and an external hard drive containing the patient data was taken from the home.

These incidents provide the opportunity to remind you that USC Policy (please see: http://fbs.usc.edu/depts/purchasing/page/2964/encrypted-laptop-devices/) requires that all laptops and mobile storage devices acquired on or after April 22, 2009, that are paid for using university funds and/or used for university business purposes must be purchased with an encryption solution. To be in compliance with this policy, laptops and mobile storage devices must be either a) delivered with built-in encryption (preferred) or b) accompanied by a software-based encryption solution for subsequent installation. Note that even if the instrument is encrypted, the best practice is to avoid storing any sensitive data on any laptop or mobile storage device.

More information about the breaches described above is available at:

http://www.msnbc.msn.com/id/48015851/ns/technology_and_science-security/t/stolen-laptop-puts-texas-cancer-center-patients-risk/

http://boston.cbslocal.com/2012/05/23/boston-childrens-hospital-reports-possible-security-breach/

http://articles.latimes.com/2011/nov/05/local/la-me-ucla-medical-data-20111105

IN THE HEADLINES: University of Missouri's Medical-School Dean to Step Down Amid Fraud Inquiry

(Source: Health Care Daily report: News Archive> 2012 > 06/05/2012 and The Columbia Daily Tribune June 1, 2012)

Robert Churchill, dean of the University of Missouri's school of Medicine, has stepped down as part of the school's response to a federal investigation into possible Medicare-billing fraud by a pair of radiology professors.

The university began investigation into possible billing irregularities after being informed by the office of the U.S. Attorney that a federal investigation was under way. The allegation states that two radiologist did not follow the Medicare Teaching Physician rules. "We believe these two doctors sometimes claimed that they had actually completed a second review of radiology exams without actually looking at the image", said Hal Williamson, vice chancellor of the MU Health System. The institution has fired the radiologists at the center of the investigation.

For questions regarding your obligations under Medicare's Teaching

Physician Rule, please call Rene Argomaniz at the Health Science Campus Office of Compliance 323-442-8588.

Forward this email

USC Office of Compliance | University Gardens Building | 3500 S. Figueroa Street | Suite 105 | Los Angeles | CA | 90089-8007