Issue 3, Fall 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.

Obama Administration Announces Ground-breaking Public-Private Partnership to Prevent Health Care Fraud

(Source: Health and Human Services Press Office)

Health and Human Services (HHS) Secretary Kathleen Sebelius and Attorney General Eric Holder today announced the launch of a ground-breaking partnership among the federal government, State officials, several leading private health insurance organizations, and other health care anti-fraud groups to prevent health care fraud. The new partnership is designed to share information and best practices in order to improve detection and prevent payment of fraudulent health care billings. Its goal is to reveal and halt scams that cut across a number of public and private payers. The partnership will enable those on the front lines of industry anti-fraud efforts to share their insights more easily with investigators, prosecutors, policymakers and other stakeholders. It will help law enforcement officials to more effectively identify and prevent suspicious activities, better protect patients' confidential information and use the full range of tools and authorities provided by the Affordable Care Act and other essential statutes to combat and prosecute illegal actions.

One innovative objective of the partnership is to share information on specific schemes, utilized billing codes and geographical fraud hotspots so that action can be taken to prevent losses to both government and private health plans before they occur. Another potential goal of the partnership is the ability to spot and stop payments billed to different insurers for care delivered to the same patient on the same day in two different cities. A potential long-range goal of the partnership is to use sophisticated technology and analytics on industry-wide healthcare data to predict and detect health care fraud schemes.

Stolen Laptop Costs Provider $1.5 Million

(Source: Hooper, Lundy & Bookman, PC)

In a sign of growing impatience with heel-dragging providers, the Department of Health and Human Services (HHS) has settled potential HIPAA violations arising from the theft of a laptop containing unencrypted health information for $1.5 million. According to the press release and a Resolution Agreement between HHS and the provider, the provider - a hospital and its related medical group - reported the theft of the laptop to HHS in April of 2010. The laptop contained patient prescriptions and clinical information. The Resolution Agreement states that HHS's investigation indicated that until late 2009, the provider had not conducted a full security risk analysis, and did not implement required privacy and security policies, procedures and

controls until 2010. The provider did not admit any HIPAA violations.

In addition to the monetary settlement, the Resolution Agreement requires the provider to comply with a three-year Corrective Action Plan (CAP). The provider is also required to appoint an independent monitor, approved by HHS, to review the provider's compliance with the CAP. The monitor must make unannounced site visits, interview workforce members, and investigate reports of noncompliance with the CAP. The monitor is to make twice-annual reports to HHS. HHS reserves the right to conduct its own reviews of the provider's compliance. The provider must also submit its own annual compliance report to HHS and the monitor.

The settlement indicates that - more than seven years after providers were supposed to be compliant with the HIPAA Security Rule - those who have not performed a risk analysis and implemented security policies and procedures can expect little sympathy if they suffer a security incident - even if they report it themselves. It also illustrates the risks of using laptops to store unencrypted health information. Although HIPAA does not mandate encryption of portable media, if this laptop had been properly encrypted, its loss would not have been reportable under federal breach reporting standards.

California Establishes Privacy Enforcement and Protection Unit

(Source: Morgan, Lewis & Bockius LLP)

On July 19, California Attorney General Kamala Harris announced the creation of a new Privacy Enforcement and Protection Unit (the Privacy Unit), which is likely to lead to more aggressive enforcement of the privacy laws applicable to all businesses that collect personal information of California residents, regardless of whether the businesses are based in the state.

The formation of the Privacy Unit follows Attorney General Harris's February 2012 announcement regarding a new privacy policy requirement for mobile application (app) operators, which requires companies to provide users with the opportunity to review and accept a privacy policy regarding their personal information before downloading an app.

This also follows the amendment of California's security breach notification statute, effective January 2012, which now requires reporting of security breaches involving more than 500 Californians to the attorney general's office. It is not coincidence that the statutory amendment and the formation of the Privacy Unit both occurred this year-it is likely that the Privacy Unit will begin investigating security breaches now reported to the attorney general's office under the amended statute.

Physicians are Currently Receiving Audit letters from Anthem Blue Cross

Anthem Blue Cross has engaged EquiClaim to benchmark providers to detect coding patterns that may suggest inappropriate upcoding by providers. EquiClaim appears to be focusing on the same codes that Medicare is currently auditing, level 4 and level 5 Evaluation and

Management Services. They state that by the terms of our contract with Anthem, we are obligated to follow the CMS guidelines for coding and documentation.

The Healthcare Compliance Program provides extensive education and monitoring to ensure our physicians are familiar with these requirements and document accordingly. As such, please contact Nancy Gonzalez at (323) 442-9061, in the Office of Compliance should you have any questions regarding the appropriate coding and documentation of your services.

Forward this email

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