OBER | KALER
Attorneys at Law

2012 Issue 12

www.ober.com

Medicaid Pays $1,700,000 to Settle HIPAA Security Violations

By: Sarah E. Swank

In its first enforcement action against a state agency, the Department of Health and Human Services (HHS) Office for Civil Rights (OCR) settled last month with Alaska's Department of Health and Social Services (DHSS) for HIPAA security violations it reported as required by HITECH. DHSS entered into a settlement agreement [PDF] and agreed to pay $1,700,000 after a USB hard drive (an electronic storage device) potentially containing electronic protected health information (ePHI) was stolen from the vehicle of a DHSS computer technician in October 2009.

The HITECH Breach Notification Rule [PDF] requires covered entities to report a breach, an impermissible use or disclosure of ePHI, of 500 individuals or more to the Secretary of HHS and the media. Smaller breaches affecting less than 500 individuals must be reported to the Secretary of HHS annually. OCR investigates each breach of 500 individuals or more reported under HITECH. In this case, OCR reviewed DHSS's written response, policies, procedures, information regarding training activities and documentation related to compliance with the Privacy and Security Rules, and conducted on-site interviews of the DHSS workforce. At the conclusion of its investigation, OCR found that DHSS did not:

- Complete a risk analysis
- Implement sufficient risk management measures
- Complete security training for DHSS workforce members
- Implement device and media controls
- Address device and media encryption

As a result, DHSS entered into a three-year Corrective Action Plan (CAP) incorporated into its settlement agreement with OCR, requiring DHSS to develop, maintain, and revise as necessary, its written policies and distribute those policies to workforce members. The minimum content of these policies must include the

following procedures:

- Tracking devices containing ePHI
- Safeguarding devices containing ePHI
- Encrypting devices that contain ePHI
- Disposal and/or re-use of devices that contain ePHI
- Responding to security incidents
- Applying sanctions to workforce members who violate these policies and procedures

In addition, DHSS is responsible for developing and submitting a risk analysis and description of risk management measures to OCR for review and approval, submitting implementation and annual reports, and designating an individual or entity with expertise in compliance with the Security Rule to be a monitor and review DHSS's compliance with the CAP. In OCR's press announcement, Leon Rodriguez, Director of OCR, cautioned, "Covered entities must perform a full and comprehensive risk assessment and have in place meaningful access controls to safeguard hardware and portable devices."