eALERT

INCompliance

February 25, 2011

HHS Announces Second Penalty for Violations of HIPAA Privacy Rule

On February 24, the Department of Health and Human Services (HHS) Office of Civil Rights (OCR) announced that General Hospital Corporation and Massachusetts General Physicians Organization, Inc. (collectively "Mass General") has entered into a settlement agreement to resolve a complaint that they violated the Health Insurance Portability and Accountability Act (HIPAA) privacy rules. As part of the settlement agreement, Mass General has agreed to pay a $1 million fine. This is the second major penalty for violation of the HIPAA privacy rules announced by OCR this week.

The incident which gave rise to the complaint was the loss of protected health information of 192 individuals. The loss occurred when a Mass General employee took home patient medical records and lost them on a subway train. The lost medical records were never recovered. After an investigation, OCR determined that Mass General had failed to adopt comprehensive written policies and procedures to ensure that PHI is protected when removed from the Mass General premises.

In addition to paying the $1 million penalty, Mass General agreed to a Corrective Action Plan (CAP) which includes the following:

1. Mass General must develop, maintain, and revise as necessary, written policies and procedures governing (i) physical removal and transport of protected health information, (ii) laptop encryption, and (iii) USB drive encryption that protect the privacy of individually identifiable information within 90 days of the CAP's effective date. The new policies and procedures must include administrative, physical, and technical safeguards to protect health information from any intentional or unintentional uses and disclosures, and a procedure for reporting violations.

2. The new policies and procedures are subject to approval by HHS.

3. Mass General must document distribution of the new policies and procedures to all workforce members, and must train all workforce members who have access to and use protected health information on the new policies and procedures within 90 days of HHS's approval of the policies and procedures.

4. Mass General must designate an individual to serve as a monitor under the CAP and who must conduct assessments of the implementation and compliance of the CAP. The assessments must include unannounced site inspections, interviews with personnel, inspections of laptops and USB drives, and review of policies and documentation at Mass General. The monitor must prepare and submit semi-annual reports to HHS of such assessments.

Earlier this week, OCR imposed the first ever civil monetary penalty on Cignet Health Plan in Maryland for violations of HIPAA, in the amount of $4.3 million. The announcement of two major penalties for HIPAA violations in one week is a clear indication that OCR has stepped up enforcement activity, and that significant complaints about violations of HIPAA will no longer be resolved with a simple order to comply. The director of OCR acknowledged this increased enforcement activity by urging health care providers to "take a close look at this agreement and recognize that OCR is serious about HIPAA enforcement."

The HIPAA regulations are complex, and managing HIPAA compliance is a difficult task in any organization, but particularly in large organizations which maintain a great deal of PHI which is accessed on a daily basis by hundreds of employees. In addition, rapidly changing technology is creating new challenges to assuring that electronic PHI is secure.

In order to avoid large penalties, it is essential that health care providers and health plans develop an active system to monitor compliance and audit their compliance program, including a periodic review and update of their policies and procedures to address new technology and organizational changes. Relying on the policies and procedures adopted when the privacy regulations became effective in 2003 is no longer sufficient to assure compliance and to avoid serious penalties.