

## **HHS imposes a \$4.3 million civil money penalty for violations of the HIPAA Privacy Rule**

Action marks first civil money penalty issued by HHS for HIPAA Privacy Rule violations

The U.S. Department of Health and Human Services' (HHS) Office for Civil Rights (OCR) has issued a Notice of Final Determination finding that Cignet Health of Prince George's County, Md., (Cignet) violated the Privacy Rule of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). HHS has imposed a civil money penalty (CMP) of \$4.3 million for the violations, representing the first CMP issued by the Department for a covered entity's violations of the HIPAA Privacy Rule.

The CMP is based on the violation categories and increased penalty amounts authorized by Section 13410(d) of the Health Information Technology for Economic and Clinical Health (HITECH) Act.

"Ensuring that Americans' health information privacy is protected is vital to our health care system and a priority of this Administration. The U.S. Department of Health and Human Services is serious about enforcing individual rights guaranteed by the HIPAA Privacy Rule," said HHS Secretary Kathleen Sebelius.

In a Notice of Proposed Determination issued Oct. 20, 2010, OCR found that Cignet violated 41 patients' rights by denying them access to their medical records when requested between September 2008 and October 2009. These patients individually filed complaints with OCR, initiating investigations of each complaint. The HIPAA Privacy Rule requires that a covered entity provide a patient with a copy of their medical records within 30 (and no later than 60) days of the patient's request. The CMP for these violations is \$1.3 million.

During the investigations, Cignet refused to respond to OCR's demands to produce the records. Additionally, Cignet failed to cooperate with OCR's investigations of the complaints and produce the records in response to OCR's subpoena. OCR filed a petition to enforce its subpoena in United States District Court and obtained a default judgment against Cignet on March 30, 2010. On April 7, 2010, Cignet produced the medical records to OCR, but otherwise made no efforts to resolve the complaints through informal means.

OCR also found that Cignet failed to cooperate with OCR's investigations on a continuing daily basis from March 17, 2009, to April 7, 2010, and that the failure to cooperate was due to Cignet's willful neglect to comply with the Privacy Rule. Covered entities are required under law to cooperate with the Department's investigations. The CMP for these violations is \$3 million.

"Covered entities and business associates must uphold their responsibility to provide patients with access to their medical records, and adhere closely to all of HIPAA's requirements," said OCR Director Georgina Verdugo. "The U.S. Department of Health and Human Services will continue to investigate and take action against those organizations that knowingly disregard their obligations under these rules."

NOTE: Individuals who believe that a covered entity has violated their (or someone else's) health information privacy rights or committed another violation of the HIPAA Privacy or Security Rule may file a complaint with OCR at <http://www.hhs.gov/ocr/privacy/hipaa/complaints/index.html>.

## **Massachusetts General Hospital settles potential HIPAA Violations**

### ***Large hospital system to improve policies and procedures safeguarding patient information***

The General Hospital Corporation and Massachusetts General Physicians Organization Inc. (Mass General) has agreed to pay the U.S. government \$1,000,000 to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule, the U.S. Department of Health and Human Services (HHS) announced today.

Mass General, one of the nation's oldest and largest hospitals, signed a Resolution Agreement with HHS that requires it to develop and implement a comprehensive set of policies and procedures to safeguard the privacy of its patients. The settlement follows an extensive investigation by the HHS Office for Civil Rights (OCR), which enforces the HIPAA Privacy and Security Rules. The HIPAA Privacy Rule requires health plans, health care clearinghouses and most health care providers (covered entities) to protect the privacy of patient information through administrative, physical and technical safeguards at all times.

"We hope the health care industry will take a close look at this agreement and recognize that OCR is serious about HIPAA enforcement. It is a covered entity's responsibility to protect its patients' health information," said OCR Director Georgina Verdugo.

The incident giving rise to the agreement involved the loss of protected health information (PHI) of 192 patients of Mass General's Infectious Disease Associates outpatient practice, including patients with HIV/AIDS. OCR opened its investigation of Mass General after a complaint was filed by a patient whose PHI was lost on March 9, 2009. OCR's investigation indicated that Mass General failed to implement reasonable, appropriate safeguards to protect the privacy of PHI when removed from Mass General's premises and impermissibly disclosed PHI potentially violating provisions of the HIPAA Privacy Rule.

The impermissible disclosure of PHI involved the loss of documents consisting of a patient schedule containing names and medical record numbers for a group of 192 patients, and billing encounter forms containing the name, date of birth, medical record number, health insurer and policy number, diagnosis and name of providers for 66 of those patients. These documents were lost on March 9, 2009, when a Mass General employee, while commuting to work, left the documents on the subway train that were never recovered.

Mass General also agreed to enter into a Corrective Action Plan (CAP), which requires the hospital to:

- Develop and implement a comprehensive set of policies and procedures that ensure PHI is protected when removed from Mass General's premises;
- Train workforce members on these policies and procedures; and
- Designate the Director of Internal Audit Services of Partners HealthCare System Inc. to serve as an internal monitor who will conduct assessments of Mass General's compliance with the CAP and render semi-annual reports to HHS for a 3-year period.

"To avoid enforcement penalties, covered entities must ensure they are always in compliance with the HIPAA Privacy and Security Rules," said Verdugo. "A robust compliance program includes employee training, vigilant implementation of policies and procedures, regular internal audits, and a prompt action plan to respond to incidents."