Patient records that were left on a subway have now cost Massachusetts General Hospital (Mass General) $1 Million. On March 9, 2009, and before HITECH's data breach notification requirements were in place and being enforced, a Mass General employee removed documents containing PHI from her bag and placed them on the seat beside her while commuting on the subway. The documents were left on the subway and never recovered. The documents included PHI on 192 patients who had been treated in Mass General's infectious disease practice, including HIV/AIDS patients. As a result of the "potential violations" of HIPAA's Privacy and Security Rule arising from this incident, Mass General entered into a Resolution Agreement with HHS. In addition to the hefty penalty, the agreement requires Mass General to implement a comprehensive corrective action plan to safeguard the privacy of its patients when PHI is removed from Mass General's facility. The plan's steps will include:

• Procedures for training work force members on safeguarding PHI taken off premises; and

• the designation of an internal monitor who will conduct assessments of Mass General's compliance with the plan and deliver semi-annual reports to HHS for a three-year period.

The press release issued by HHS notes that Mass General is one of the nations' oldest and largest hospitals. It also states that "[w]e hope the health care industry will take a close look at this agreement and recognize that OCR is serious about HIPAA enforcement."

The Mass General penalty came on the heels of HHS's imposition of a $4.3 Million penalty on Cignet Health, the first civil monetary penalty issued under HIPAA's privacy rule. Cignet, of Prince George's County, MD, was found to have violated 41 patients' right by denying them access to their own medical records when requested between September 2008 and October 2009. Each of those patients then filed complaints with HHS, based on HIPAA's privacy rule, which requires covered entities to provide patients with copies of their records within 30 days (and no later than 60 days) of a patient's request. HHS found that Cignet's failure to cooperate was due to willful neglect under the Privacy Rule. Cignet was fined $1.3 million for failure to turn over the records and

another $3 million ($1.5 Million for both calendar years 2009 and 2010) for failure to cooperate with HHS's investigation, for a total of $4.3 Million.

What message is HHS sending with these large penalties involving a small number of patients? Is the high sensitivity of the information involved in the Mass General breach driving the penalty amount? Are these types of fines going to be commonplace? Whatever the reasons behind the penalties, both penalties show that HHS clearly intends to take a tough stance on violations of the privacy and security rules. HHS is flexing its muscles pursuant to the increased penalty amounts now authorized under HITECH. In fact, Cignet's fine would likely have been even higher, but for the calendar year limit of $1.5 Million per violation.

A copy of the HHS press release relating to the Mass General fine is available here:

http://www.hhs.gov/news/press/2011pres/02/20110224b.html

The Mass General resolution agreement and action plan can be found here:

http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/massgeneralra.pdf

HHS's notices of proposed determination and final determination relating to Cignet are available here:

http://www.hhs.gov/ocr/privacy/hipaa/news/cignetnews.html

Please contact us if you have any HIPAA/HITECH or other privacy questions.

Ted

Theodore J. Kobus, Esq.

Chair, Technology, Media & IP Litigation Practice Group

1845 Walnut Street
Philadelphia, PA 19103
Main: (215) 575-2600
Direct: (215) 575-2713
Fax: (215) 575-0856

- website
- e-mail
- bio