Careless Name-dropping Costs Health System $2.4M in HIPAA Settlement

A large health system in Texas has learned some Health Insurance Portability Accountability Act (HIPAA) lessons it's not likely to forget, or repeat…and has learned them the hard way, to the tune of $2.4 million. It would, of course, behoove all health systems to take notice and thereby avoid learning the same lessons in the same way.

Houston-based Memorial Hermann Health System (MHHS) is a not-for-profit health system that includes more than a dozen hospitals, more than two dozen rehabilitation centers, and more than 24,000 employees. The U.S. Department of Health and Human Services Office for Civil Rights (OCR) recently announced a settlement against MHHS that includes not only the aforementioned financial penalty, but also a corrective action plan that will require training and documentation of the health system's program to achieve ongoing HIPAA compliance.

Authorities involved when employee suspected fraud

In the fall of 2015, a patient visiting one of MHHS's facilities allegedly gave office staff a fake insurance card. The MHHS emp called the authorities, which resulted in the patient's arrest.

Up to this point, MHHS had still been HIPAA-compliant; disclosing protected health information (PHI) in conjunction with effor law enforcement to address suspected criminal activity is allowed under the Act.

However, MHHS didn't stop there. Without permission from the patient in question, the health system published a press relea that identified the individual (in the title, no less) and that made it to more than a dozen media sources. The health system's o website featured a statement that included the patient's name. Additionally, MHHS inappropriately name-dropped when its ag divulged the patient's identity in three different meetings (with a state senator, state representatives, and an advocacy group).

Violators include high-level representatives

What perhaps makes these mistakes even harder to swallow is that they can't be chalked up to inexperience; senior leadersh was allegedly involved in these repeated privacy blunders. MHHS did not have the right under HIPAA to continue to share PH beyond the alerting of the authorities to what an employee believed was a fraudulent insurance ID card. Further, the OCR wa pleased with the absence of timely evidence that demonstrated offending employees were disciplined over the violations (thou MHHS stated that the staff members did receive disciplinary action).

The corrective action plan stipulated in the settlement will require the health system to implement a program for protecting patient privacy and train all employees for HIPAA compliance.

Cooperating with law enforcement and protecting patient privacy not mutually exclusive

“This case reminds us that organizations can readily cooperate with law enforcement without violating HIPAA,” said HHS Office for Civil Rights director Roger Severino in a statement, “but that they must nevertheless continue to protect patient privacy when making statements to the public and elsewhere.”

According to the OCR, in 2015 the Office was in receipt of more than 17,000 HIPAA privacy rule complaints. So far only around 1,000 of those have made it under the government’s microscope. The OCR also notes that complaints in this category have continued to uptick from 2003 to 2014 (stats are not available prior to 2003); the period between 2014 and 2015 showed a slight decrease in number of privacy complaints.