COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 19, Number 6. June 05, 2019 $3 Million Settlement Demonstrates Need for Quick Breach Management

By Theresa Defino

From the government's telling, the new $3 million settlement between the HHS Office for Civil Rights (OCR) and Touchstone Medical Imaging LLC of Franklin, Tennessee, sounds like a lesson in what not to do if you have a HIPAA breach.

In short, you keep digging when you learn there might be a breach, and you'd better have your house in order if it turns out to be a reportable one.

The settlement, announced May 6, could be the last of the big-dollar agreements; it was signed in early April, just weeks before OCR Director Roger Severino announced that, effective immediately, the agency was shaving its annual maximum penalties ("Easy Win for MD Anderson? OCR Drops Annual Caps, Issues Warning on Right-of-Access Denials," *RPP* 19, no. 5).

Then again, OCR is maintaining the highest level of $1.5 million per year (per identical violation when due to willful neglect not corrected within 30 days), which perhaps is apt in this instance.

The Touchstone settlement is the first OCR signed this year. It ended 2018 with a total of $28.7 million in penalties imposed or agreed to (but not collected), a record ("OCR Piggybacks on Another Calif. Settlement, Adds $3M From Cottage Health to 2018 Total," *RPP* 19, no. 3).

Breach Delay Prompts Settlement

OCR has not collected $4.458 million a court imposed on the University of Texas MD Anderson Cancer Center, as it has appealed and its case is currently pending in U.S. District Court for the Southern District of Texas ("Should 'State' Agencies Be Exempt From HIPAA? MD Anderson Says Yes," *RPP* 19, p. 5).

According to its website, Touchstone "has over 1,000 employees and operates 60 outpatient imaging centers across Texas, Colorado, Oklahoma, Florida, Nebraska, Arkansas and Montana." Despite its many years in operation—it was founded in 1991—it was allegedly roundly noncompliant with the security rule requirements in addition to its handling of the May 2014 breach that got OCR's attention.

On May 9 of that year, someone tipped OCR off that Social Security numbers of some Touchstone patients were exposed "via an insecure file transfer protocol (FTP) web server." Three days later, OCR confirmed this was true and notified Touchstone that it was beginning an investigation into the breach.

According to OCR, the FBI notified Touchstone on May 9 of the exposure—the same day OCR was alerted. Apparently referring to Touchstone's 2014 breach notification, OCR said in its announcement that "Touchstone initially claimed that no patient [protected health information] PHI was exposed."

Ultimately, OCR concluded that PHI of 307,839 individuals whose "name, date of birth, phone number, address (and in some instances, social security numbers)" were exposed. OCR said its investigation "determined that the server was configured to allow anonymous FTP connections to a shared directory."

But, at least at first, Touchstone didn't realize the extent of the problem.