

## Report on Medicare Compliance Volume 30, Number 32. September 13, 2021

### Hospital Settles FCA Case Filed by CO Over Modifiers; Make Sure People 'Feel Heard'

---

By Nina Youngstrom

John Peter Smith (JPS) Hospital in Fort Worth, Texas, agreed to pay \$3.3 million to settle false claims allegations in a case with a hot risk area, a compliance officer-turned-whistleblower and a self-disclosure. Erma Lee, the former director of compliance, alleged the hospital improperly billed for three modifiers and didn't return the overpayments even after she alerted executives, according to her 2018 False Claims Act (FCA) complaint.<sup>[1]</sup> During the subsequent Department of Justice investigation, the hospital voluntarily repaid its Medicare administrative contractor \$438,673, according to the settlement, which was announced by the U.S. Attorney's Office for the Northern District of Texas Aug. 27.<sup>[2]</sup>

The government alleged JPS submitted Medicare claims with "inappropriate or otherwise unjustified" modifiers 25, 59 and XU from 2008 through 2016, the settlement states. The U.S. attorney's office declined to intervene in the lawsuit, and the hospital corrected the modifier problem after the whistleblower separated from the hospital, said its attorney, Jason Mehta.

Modifiers allow providers to bypass National Correct Coding Initiative billing edits that otherwise prevent improper payments for evaluation and management (E/M) services and procedures when they're not separately payable. They've been under the microscope of Medicare watchdogs for years, with the HHS Office of Inspector General (OIG) finding high error rates for certain modifiers. In April, OIG added an audit to the Work Plan of modifier 25 on dermatologists' claims for E/M services, while CMS produces comparative billing reports on modifier 25.<sup>[3]</sup>

### Some CCOs Worry About Personal Liability

The JPS case is also the latest FCA lawsuit with a compliance professional as the whistleblower. It raises questions about the implications of the person who is responsible for helping identify problems internally filing a whistleblower complaint when they're rebuffed.

"I've known people who have gone down that road," said Kelly Sauders, a partner in Deloitte Risk & Financial Advisory. One compliance officer spent two years calling attention to problems at their organization, but leadership and counsel didn't seem sufficiently responsive. As the compliance officer's anxiety and depression mounted, along with worry about personal liability, the compliance officer eventually filed the whistleblower lawsuit, which settled, Sauders said. "It takes a toll on someone to do that. This person had to step away from the industry and do something different." In another case, the compliance officer didn't try to resolve problems internally, Sauders said. "There are different stories and different circumstances."

From her work on false claims cases, Sauders has learned the value of paying close attention to people's behavior in interviews and to their history. There are warning signs in the number of times they've complained about the same problem, and leaders are cavalier at their own risk, she said. "Sometimes it's obvious when people are nervous and the way they say certain things," Sauders explained. It's a red flag if the employee expressed

---

concern about an issue several times and retained documentation “and they feel like they have done what they can and start to believe they have personal risk,” she said. “Leaders should quickly determine who they can talk to, make sure the person feels fully heard and, within reason, knows that leadership is taking steps to address the concern.” Even though compliance officers and senior leaders are often unable to share details of an investigation, they can follow up with the person raising the concern to check in and reassure that actions are being taken. “Organizations that help people be heard and try to share what they can help mitigate their risk,” Sauders said.

This document is only available to subscribers. Please [log in](#) or [purchase access](#).

[Purchase](#) [Login](#)