COSMOS
Navigate the Compliance Universe

Compliance Today - March 2023

**Axel Del Rosario Rotger** (axel.delrosariorot@jhsmiami.org, linkedin.com/in/axel-del-rosario-rotger-jd-chc-b3bb1215a/) is Director of Policy Administration & Compliance Officer at Jackson Health System, Miami, FL.

# The investigation before qui tam

by Axel Del Rosario Rotger, JD, CHC

On the topic of human ambition, Ecclesiastes 1:9 is credited with the saying: "What has been will be again, what has been done will be done again; there is nothing new under the sun." This was allegedly said in the mid-10th century B.C.

Healthcare fraud is certainly not new. However creative a fraud scheme may seem, chances are it's been done. Healthcare fraud is a known high-risk area that affects the healthcare industry, government officials, taxpayers, insurers, premium-payers, and trusting patients who are at significant risk of injury in some fraud schemes. Healthcare attorneys, compliance officers, and operators around the nation have the insurmountable task of spotting what these fraud schemes look like and how they are being carried out so they can create and implement oversight processes to detect and prevent them. Additionally, if left unattended, healthcare fraud can potentially cause a healthcare institution's financial demise due to the strength of federal laws surrounding this subject and the hefty penalties accompanying them.

Healthcare fraud, like any fraud, demands that false information be represented as truth. An all-too-common healthcare fraud scheme involves perpetrators who exploit patients by entering their medical records' false diagnoses of medical conditions they do not have or more severe conditions than they actually have. This is done so fraudulent insurance claims can be submitted for payment. Unless and until this discovery is made, these false or inflated diagnoses become part of the patient's documented medical history.

## Upcoding

Probably the most common method of defrauding the government is *upcoding*. This involves billing for services that were either never rendered or billing for one service when a similar but cheaper service was actually provided. Perpetrators target vulnerable patients, and while in some ways every patient is somewhat vulnerable and could become a victim of fraud, a strong case can be made for psychiatric and mental health patients as being uniquely vulnerable—especially when dealing with Medicare or Medicaid as their health insurance.

Government enforcement authorities are paying extra attention to billing and payments after the passing of The Payment Integrity Information Act of 2019, which requires the Centers for Medicare & Medicaid Services (CMS) to periodically review programs it administers, identify programs that may be susceptible to significant improper payments, estimate the number of improper payments, and report on the incorrect payment estimates.[1]

The Center for Program Integrity (CPI)—CMS's centralized entity for Medicare and Medicaid program integrity issues—has experienced an increase in its resources over time, and the agency has established work groups and

interagency collaborations to extend its capacity. For example, CMS allocated additional staff to CPI after Congress provided additional funding. CPI's full-time equivalent positions increased from 177 in 2011 to about 492 in 2021. In total, Medicare improper payments were estimated to be $43 billion in fiscal year 2020[2] compared to $57.4 billion for fiscal year 2019.[3]

A highly effective method to combat healthcare fraud is reporting suspicious activity to an insurer or government payer. Patients are notified by their insurers through the explanation of benefits statements about treatments received and instructed to communicate any discrepancies that may arise with them. But what happens when it is not the patient who notices the discrepancies but a current or former healthcare facility employee?