DOJ'S INCREASED USE OF DATA ANALYTICS TO PURSUE CRIMINAL AND CIVIL ENFORCEMENT ACTIONS

September 2021

As McDermott partners Julian André and Justin Murphy explained in their recent *Bloomberg Law* article, the DOJ's expanded and effective use of data analytics is a game changer, and will lead to increased criminal and civil enforcement activity across the board. In the healthcare context, DOJ and HHS-OIG have repeatedly emphasized the importance of using data analytics to identify fraud and abuse. And DOJ's use of data analytics has already led to a significant increase in federal False Claims Act (FCA) cases initiated directly by the DOJ, as opposed to via qui tam whistleblower complaints. Indeed, DOJ initiated 100 more FCA cases in 2020 than it did in 2019, resulting in the most non-qui-tam FCA cases filed in nearly 30 years. McDermott expects the number of data-driven FCA fraud investigations to continue to increase, particularly as the government continues to investigation potential fraud associated with the CARES Act, the Provider Relief Fund, and the COVID-19 pandemic.

There are a number of measures hospitals and health systems should take in response to the DOJ's and HHS-OIG's increased focus on data analytics:

1. First, hospitals and health care systems should understand what data is readily available to the government and how the government can use such data to identify potentially fraudulent conduct. For example, the DOJ and HHS-OIG can easily compare claims and other transactions data – both current and historical – from a particular hospital to nationwide statistics or other similar facilities to identify suspicious billing patterns and other outliers. The DOJ and HHS-OIG also have access to vast amounts of other data sources, including public records databases, bid submissions, and non-public financial information obtained by the Financial Crimes Enforcement Network (FinCEN), all of which can be utilized to identify and investigate potential health care fraud schemes.
2. Second, hospitals and health systems should consider incorporating data analytics into their own audit and compliance programs to minimize enforcement risk. For example, a comprehensive data analytics program could help companies identify and address potential overpayments, upcoding or billing issues, procurement fraud, and even Anti-Kickback Statute or Stark law concerns, among others. Identifying and auditing these potential risks early on could prevent healthcare companies from becoming entangled in costly government investigations and prosecutions. Hospitals and health systems should continue to monitor high risk areas, evaluate whether all data relating to those risk areas is actually being collected, and then put in place systems to ensure that the data collected is being effectively monitored and analyzed to identify any potential errors and/or misconduct.
3. Third, to the extent healthcare companies find themselves subject to a criminal prosecution or government enforcement actions, defense counsel may take a number of reactive measures.

Among other things, defense counsel may seek discovery regarding the government's use of data analytics and challenge any improper collection or use of the underlying data. Defense counsel should consider conducting their own data analysis to prepare an effective defense strategy. Indeed, data analytics can be instrumental in helping hospitals and health systems effectively respond to a government enforcement action.

VISIT **MWE.COM/HHS** FOR MORE RESOURCES TO SUPPORT YOUR ORGANIZATION'S BUSINESS AND COMPLIANCE GOALS

McDermott Will & Emery