COSMOS
Navigate the Compliance Universe

# Report on Medicare Compliance Volume 31, Number 37. October 10, 2022
# Fraud Enforcers Use Data 'To Fight Fire With Fire,' CCOs Need Access to it, Officials Say

By Nina Youngstrom

Data analysis and other technology have changed the nature of fraud and fraud-fighting, according to Christi Grimm, the HHS Inspector General, and Kenneth Polite, the assistant attorney general for the criminal division at the Department of Justice (DOJ).

"Data has allowed us to fight fire with fire," Grimm said Sept. 28 at the American Health Law Association's Fraud and Compliance Forum in Baltimore.[1] "We have made a tremendous investment in data capability. We have to keep pace with what the fraudsters are doing."

At the same time, data is an essential tool for compliance officers. "You need to have a seat at the table and access to the data your organization has" and be able to partner with IT and internal audit, said Polite, a former compliance officer. "The siloed walls need to be broken down and your company's leadership needs to understand" that's a DOJ expectation.

Grimm explained how "the infusion of technology" has allowed local frauds to go national, with far more dollars in play and more beneficiaries at risk. Durable medical equipment (DME) fraud "is instructive," she said. DME schemes previously relied on brick-and-mortar locations, with local TV ads and telemarketing. "It used to be a self-contained cell. You had to steal provider numbers and beneficiary numbers to commit fraud. Now you can go to the dark web and purchase the information and hire call centers to do telemarketing nationwide," Grimm said. "The effect is something that is bigger, fast moving, more efficient, all meant to maximize ill-gotten gains through the use of technology."