COSMOS
Navigate the Compliance Universe

Report on Medicare Compliance Volume 28, Number 1. January 14, 2019
Outlook 2019: Danger and Opportunity Are Ahead With Cyber, Stark, Payments; Same Compliance Tools Apply

By Nina Youngstrom

The federal government may be slowed by the shutdown, but it doesn't foreshadow the pace of compliance and enforcement in 2019. Payment changes, technology advances and new enforcement targets will keep health care organizations moving fast, and there will be no break from the challenges to their claims from Medicare and commercial payers.

New payment rules that took effect Jan. 1 will put reimbursement and compliance pressure on hospitals, including site neutrality, which CMS is expected to push even further this year, compliance officers and attorneys say. Cybersecurity will become more of an enforcement target and focus more on patient harm. False Claims Act (FCA) cases based on the Stark Law may favor the structure of compensation over fair market value. More organizations are expected to revisit their conflicts of interest and conflicts of commitment policies in the wake of the scandal at Memorial Sloan Kettering Cancer Center. And the use of data will drive enforcement and health care innovation, prompting compliance officers to adapt their skill sets accordingly. These and other predictions —on audits, telehealth, export control and more—indicate 2019 will be anything but dull.

"It's not one of those ease-back-into-it years," says attorney Sara Kay Wheeler, with King & Spalding in Atlanta, Georgia.

On the audit front, hospitals will thrust and parry more often with Medicare Advantage (MA) plans and commercial payers and have Special Needs Plans to contend with if they accept their contracts. Recovery audit contractors (RACs) may get in your face more after slowly gearing up since their second five-year contracts went into effect in 2017, and in December, CMS posted a number of complex RAC audits under consideration.

Whatever the risk, compliance tenets are the rock, says Margaret Hambleton, chief compliance officer at Dignity Health in California. "Even though health care delivery and technology seem to be moving at the speed of light, that doesn't change the fact that we as compliance officers need to focus on and be really good at the fundamentals, including assessing risk, providing education, ensuring policies are in place to safeguard the organization, and developing new methods to monitor new technologies, service lines, and delivery models." Hambleton says compliance officers should continue to concentrate on serving patients, taxpayers and the community at large. "As long as we focus on the fundamentals, we will be fine regardless of how the world changes around us."

And there could be some monster changes. 2019 may be a watershed year for Medicare guidance. As much as that sounds like hyperbole, the U.S. Supreme Court has accepted a case that could defang CMS guidance (e.g., Medicare manuals) and subregulatory guidance (e.g., transmittals), says Washington, D.C., attorney Andy Ruskin, with Morgan Lewis. If the Supremes rule a certain way, all changes would have to be made through notices of proposed and then final rulemaking, he says. "It may drastically change the way CMS regulates." The case is between CMS and a class of hospitals (with Allina Health Services in Minnesota the lead named plaintiff), and concerns the way CMS changed the formula for disproportionate share hospital payments. The calculation

includes Medicare Part A beneficiary days in the "Medicare proxy" part of the formula. The controversy centers on whether the proxy also can include Medicare Part C enrollee days. When CMS sought to include those days in a 2013 regulation, it attempted to apply it retrospectively to 2012 payments, claiming this policy was just an "interpretive rule" that didn't need to go into effect only prospectively, Ruskin says.

The hospitals sued CMS, losing in federal district court but winning at the U.S. Court of Appeals for the D.C. Circuit in an opinion written by then-appellate court judge Brett Kavanaugh. His decision said that including Part C days in the Medicare proxy "represents a change in HHS's standards," which means notice and comment are required, according to the Medicare Act. In other words, unlike other agencies, CMS can't benefit from less formal interpretive rules, the decision stated. Oral arguments are scheduled for Jan. 15, Ruskin says. "This is an important case to watch," he notes. Depending on how the Supreme Court rules, "the guidance the agency provides without notice and comment would be the agency's view. It would not be a binding statement" unless CMS put it into a regulation.

FCA Enforcement: Full Steam Ahead

Add that to the potential elimination of the Affordable Care Act (ACA), which was struck down in its entirety Dec. 14 by a federal judge and is headed for appeal, and this could be a chaotic year for health care because the ACA has a lot of compliance-related and enforcement provisions (*RMC 12/24/18, p. 5*).

But FCA enforcement will be full steam ahead, as it has for decades, lawyers say. Why mess with success in the government's eyes? On Dec. 21, the Department of Justice (DOJ) announced it obtained $2.8 billion in civil fraud and false claims during the fiscal year that ended Sept. 30, 2018. Of that amount, $2.5 billion came from the health care industry, making 2018 the ninth consecutive year civil health fraud settlements topped $2 billion.

Expect some twists. "You will see continued growth in government-initiated False Claims Act cases" vs. whistleblower-initiated cases, says former HHS Office of Inspector General senior attorney David Blank, now with Quarles & Brady in Washington, D.C. "Over the past three years, the number of non-qui tam False Claims Act cases grew by 120%. That's indicative of the government's use of data analytics to apply the enforcement priorities."

HHS Report Will Focus HIPAA on Safety

Health care will, again, be the main source of FCA recoveries, says former Acting Attorney General Stuart Gerson, an attorney with Epstein, Becker & Green in Washington, D.C. But new roads will be traveled. "The single biggest new enforcement effort will be in the area of cybersecurity preparedness. The OIG is likely to pursue enforcement of the recent HHS guidelines regarding cyber preparedness, and there will be a significant emphasis on pursuing internet of things cases with respect to medical devices," says Gerson. The HHS's Dec. 28 guidelines, *Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients*, which were developed with industry partners, presents cybersecurity as baked into health care delivery: "To adequately maintain patient safety and protect our sector's information and data, there must be a culture change and an acceptance of the importance and necessity of cybersecurity as an integrated part of patient care." The report also identifies the five top cybersecurity risks—phishing (*RMC 12/10/18, p. 1*); ransomware; loss or theft of equipment or data; insider, accidental or intentional data loss; and attacks against connected medical devices that may affect patient safety —and describes strategies for reducing them.

The guidance will change the conversation and influence enforcement, although it's still just guidance, says attorney Jami Vibbert, with Venable in New York City. "The number of times that patient safety and patient health are mentioned is incredible," she says. "There is going to be a shift in the way people think about privacy and security. Until now, all the laws have been focused on protecting data. Now the focus is shifting to other

types of non-data harm caused by attacks like ransomware and attacks that affect connected medical devices. This is an indication the HIPAA security rule will be used not only for failing to protect information but for failing to protect patient health and safety."