Top Government Enforcement Priorities in the Health Care Space

Scott R. Grubman

Fiscal year (FY) 2017 marked the eighth year in a row that the U.S. Department of Justice (DOJ) recovered over $2 billion from False Claims Act (FCA) matters within the health care industry alone.[1] In fact, since 2000, there have only been two years in which the DOJ has not recovered over $1 billion from health care providers under the FCA, and in one of those two years, they came very close (in 2000, the DOJ recovered over $932 million).[2]

The vast majority of FCA recoveries in health care have come from *qui tam* actions, which allow private whistleblowers to bring suit in the name of the United States and, as a reward for doing so, collect anywhere between 15 and 30 percent of the government's final recovery, plus attorneys' fees and costs.[3] In fact, in FY 2017, over 99 percent of the DOJ's recovery (or $2.44 billion) came from *qui tam* actions.[4]

This article will explore the government's recent top enforcement priorities within the health care space and provide a forecast as to what those priorities might be in the foreseeable future.

Scott R. Grubman is a partner with the law firm of Chilivis, Cochran, Larkins & Bever LLP in Atlanta, Georgia, where he represents health care providers of all types and sizes in connection with government investigations, False Claims Act litigation, and various other compliance-related matters. He can be reached at sgrubman@cclblaw.com.

The Statutes

False Claims Act[5]

Before discussing the government's priorities within health care enforcement, it is important to discuss the three main tools that the federal government utilizes in its enforcement activities. The main tool is the FCA, which penalizes any person who, among other things:

- Knowingly presents, or causes to be presented, a false or fraudulent claim for payment or approval;
- Knowingly makes, uses, or causes to be made or used, a false record or statement material to a false or fraudulent claim; or
- Knowingly conceals or knowingly and improperly avoids or decreases an obligation to pay or transmit money or property to the government.[6]

Although the FCA is not specific to health care, but instead applies to any person or entity that submits claims for payment to the federal government (*e.g.*, defense contractors, universities, etc.), the vast majority of activity under the FCA focuses on health care providers. For example, in FY 2017, the DOJ recovered a total of $3.7 billion under the FCA, with $2.4 billion of that from health care matters.[7] This is not surprising considering that the percentage of the country's gross domestic product attributable to health care is fast approaching 20 percent.[8]

Most health care FCA cases are premised upon allegations that the defendant submitted claims to a federal health care program (mainly Medicare, Medicaid, or Tricare) that were in some way false or fraudulent. Typically, the government alleges that the service billed for (a) was not performed at all; (b) was performed but was not medically necessary; or (c) failed to meet one of the myriad of rules and regulations promulgated by federal regulators, such as the Centers for Medicare & Medicaid Services (CMS) or one of its contractors. If the falsity was "material" to the government's decision to pay the claim (defined by the FCA as "having a natural tendency to influence, or be capable of influencing, the payment or receipt of money or property"),[9] then submission of that claim could violate the FCA if done so "knowingly," which means with actual knowledge, or in deliberate ignorance and/or reckless disregard of the truth or falsity of the information.[10] Importantly, the FCA does not require proof of specific intent to defraud.[11]

A less utilized—but equally important—provision of the FCA makes it unlawful to knowingly retain a federal health care program overpayment.[12] Known as the "Reverse False Claims" provision, it combines with the 60-day rule (passed as part of the Patient Protection and Affordable Care Act in 2010) to provide that if a health care provider knowingly retains an overpayment for more than 60 days after the provider identifies and quantifies that overpayment, the provider is in violation of the FCA, even if the provider first obtained the overpayment through absolutely no fault of its own.[13]

The reason the FCA is the federal government's favorite "fraud"-fighting tool is in large part due to the draconian penalties that it carries. Not only does a violation of the FCA entitle the government to recover three times the amount of reimbursement for the claims at issue ("treble damages"), but it also calls for penalties of between $11,181 and $22,363 *per claim*.[14] Violations of the FCA could also result in very serious administrative sanctions, including but not limited to exclusion from federal health care programs.[15]

The Stark Law[16]

Another of the powerful tools in the federal government's fraud enforcement tool chest is the Stark law. The Stark law generally prohibits a physician from referring certain "designated health services" to an entity if that physician (or an immediate family member of the physician) has a financial relationship with that entity.[17] The Stark law also prohibits the entity that is receiving the referral (*e.g.*, a hospital) from submitting a claim for such a service to Medicare or Medicaid.[18]

Unfortunately, most of the definitions of Stark's key terms are fairly broad. For example, "designated health services" is defined to include: clinical laboratory services; physical and occupational therapy, and outpatient speech-language pathology services; radiology and certain other imaging services; radiation therapy services and supplies, durable medical equipment and supplies; parenteral and enteral nutrients, equipment, and supplies; prosthetics, orthotics, and prosthetic devices and supplies; home health services; outpatient prescription drugs; and inpatient and outpatient hospital services.[19]

The term "financial relationship," as used in the Stark law, is also broadly

defined to include both direct or indirect ownership or investment interests in the DHS entity or a direct or indirect compensation arrangement with such an entity.[20] "Compensation arrangement," in turn, is also broadly defined as "any arrangement involving remuneration, direct or indirect, between a physician (or a member of the physician's immediate family[21]) and an entity."[22] Not surprisingly, "remuneration" is also broadly defined as "any payment or other benefit made directly or indirectly, overtly or covertly, in cash or in kind."[23]

Thankfully, the Stark law contains numerous exceptions to its broad prohibition. Because the Stark law is a "strict liability" statute (meaning that a provider can violate it without any ill intent or requisite knowledge), an arrangement must fall squarely within an applicable Stark law exception for a provider to avoid potential liability. A few of the most common Stark law exceptions include:

- *Rental of office space or equipment:* Payments for the use of office space or equipment do not constitute a "financial relationship" under the Stark law so long as certain requirements are met, including, among other things, that the lease be set out in a signed writing with a duration of at least one year; not exceed what is reasonable and necessary for the legitimate business purpose of the arrangement; that the rental charges be set in advance and consistent with fair market value and not be determined in a matter that takes into account the volume or value of referrals or other business generated between the parties; and that the arrangement is commercially reasonable.[24]
- *Bona fide employment relationships:* Any amount paid by an employer to a physician (or immediate family member) who has a *bona fide* employment relationship with the employer for the provision of services is exempted from Stark's definition of "financial relationship," so long as the employment is for identifiable services; the amount of the remuneration under the employment is consistent with fair market value and is not determined in a manner that takes into account (directly or indirectly) the volume or value of any referrals by the referral physician; and that the remuneration is provided under an arrangement that would be commercially reasonable even if no referrals were made to the employer.[25]
- *Personal service arrangements:* Similarly, remuneration from an entity under an arrangement to a physician or his immediate family member is exempted from Stark's general prohibition if the arrangement is, among other things, set out in a signed writing; covers all of the services to be furnished to the entity; the aggregate services covered by the arrangement do not exceed those that are reasonable and necessary for the legitimate business purposes of the arrangement; the duration of the arrangement is at least one year; and the compensation under the arrangement is set in advance, does not exceed fair market value, and is not determined in a manner that takes into account the volume or value of any referrals or other business generated between the parties.[26]

Violations of the Stark law can lead to various administrative sanctions, including but not limited to, exclusion from federal health care programs and massive per-claim penalties.[27] Moreover, claims submitted in violation of the Stark law are considered "false" under the FCA.[28]

The Anti-Kickback Statute[29]

A third major tool that the federal government utilizes to fight fraud, waste, and abuse affecting federal health care programs is the anti-kickback statute (AKS).[30] The AKS makes it unlawful to knowingly and willfully solicit, receive, offer, or pay any remuneration (including any kickback, bribe, or rebate) directly or indirectly, overtly or covertly, in cash or in

kind, in return for referring, purchasing, leasing, ordering, or arranging for any item or service payable by a federal health care program.[31] The AKS is a felony criminal statute, carrying a potential maximum penalty of 10 years in prison and a $50,000 fine per violation.[32] The AKS also carries with it potential administrative sanctions, including exclusion and civil monetary penalties.[33] Finally, a claim that is tainted by a violation of the AKS is considered "false" under the FCA.[34] Unlike the Stark law, the AKS is not "strict liability;" instead, a person must act "knowingly and willfully," generally meaning with some sort of unlawful intent. A person, however, need not have actual knowledge of the AKS itself or specific intent to violate the AKS.[35]

Similar to the Stark law's statutory and regulatory exceptions, the AKS has various safe harbors that protect certain types of arrangements from prosecution or civil enforcement. A few common safe harbors include space and equipment rental, personal services and management contracts, and the sale of a physician practice.[36] Unlike the Stark law's exceptions, which are mandatory in nature, the AKS safe harbors are voluntary. In other words, the fact that an arrangement does not fit squarely within an AKS safe harbor does not automatically mean that the arrangement violates the AKS.

Recent Enforcement Priorities

With that background, the remainder of this article will address both recent enforcement priorities within the health care space, as well as possible priorities on the horizon.

Opioid Fraud and Abuse

Unquestionably, the government's current top health care enforcement priority is opioid fraud and abuse. Perhaps the first public sign of this initiative came in July 2017, when the DOJ announced the largest health care fraud takedown in history, charging more than 400 defendants in 41 federal districts with participating in fraud schemes related to federal health care programs.[37] According to the DOJ's press, nearly one-third of the defendants charged in the takedown were charged in schemes related to prescribing and dispensing opioid and other narcotic drugs.[38]

The following month, the DOJ announced the creation of the Opioid Fraud and Abuse Detection Unit, which, according to Attorney General Jeff Sessions, will "focus specifically on opioid-related health care fraud using data to identify and prosecute individuals that are contributing to this prescription opioid epidemic."[39] The Opioid Fraud and Abuse Detection Unit will include 12 experienced Assistant United States Attorneys from various offices around the country, who will be fully funded for a three-year term to focus exclusively on investigating and prosecuting fraud related to prescription opioids, including pill mills and pharmacies that unlawfully divert or dispense prescription opioids for unlawful purposes. The DOJ chose 12 districts to take part in the Unit's pilot program: the Middle District of Florida, Eastern District of Michigan, Northern District of Alabama, Eastern District of Tennessee, District of Nevada, Eastern District of Kentucky, District of Maryland, Western District of Pennsylvania, Southern District of Ohio, Eastern District of California, Middle District of North Carolina, and Southern District of West Virginia.

According to the DOJ, data analysis will allow federal authorities to obtain important information related to prescription opioids, including identifying outlier prescribers, determining how many of a prescriber's patients die due to an opioid overdose, and tracking pharmacies that dispense disproportionately large amounts of opioids.[40] The Fraud and Abuse Detection Unit will include multiple agencies, including the DOJ, Federal Bureau of Investigation (FBI), Drug Enforcement Administration (DEA),

U.S. Department of Health and Human Services (HHS), and various state and local law enforcement agencies.[41]

Similarly, in January 2018, the DOJ announced a DEA surge to focus on pharmacies and prescribers who dispense unusual or disproportionate amounts of drugs.[42] Several months later, on April 2, 2018, the DOJ announced the results of that surge. Specifically, according to the DOJ, in a 45-day period, DEA personnel analyzed 80 million transaction reports from DEA-registered manufacturers and distributors, as well as reports submitted on suspicious orders and drug thefts and information shared by other federal agencies.[43] This surge led to 28 arrests, 54 other enforcement actions, including the execution of warrants, and 283 administrative actions, including suspensions of DEA registrations.[44]

Additionally, in late February 2018, the DOJ announced the creation of the Prescription Interdiction and Litigation (PIL) Task Force.[45] According to the DOJ, the PIL Task Force "will aggressively deploy and coordinate all available criminal and civil law enforcement tools to reverse the tide of opioid overdoses in the United States, with a particular focus on opioid manufacturers and distributors."[46] The Task Force is set to include senior officials from the DOJ, United States Attorney's Offices, and the DEA.[47]

Stark and AKS

Although opioid fraud and abuse enforcement has taken center stage in government enforcement, the DOJ and Office of Inspector General (OIG) have made clear that Stark and AKS enforcement is still a top priority. For example, in FY 2017, the DOJ continued to enter into high-dollar resolutions of Stark and AKS investigations. For example:

- In June 2017, the DOJ announced a settlement with Pacific Alliance Medical Center and its parent companies, which agreed to pay $42 million to resolve allegations brought by a whistleblower that they violated the Stark law and AKS. Specifically, the *qui tam* lawsuit alleged improper payments to referring physicians in the form of office space rental payments that were above fair market value and marketing arrangements that allegedly provided undue benefits to physician practices.[48]
- In September 2017, the DOJ announced that MediSys Health Network agreed to pay $4 million to resolve a *qui tam* suit filed by a physician, who alleged various Stark law violations. Specifically, the suit alleged that the hospital violated the Stark law by, among other things, offering office space for rent that was below fair market value and included free janitorial services, utilities, stationary, collection of medical waste, subsidized parking for patients, phone, fax, and pager services.[49]
- In December 2017, 21st Century Oncology agreed to pay the DOJ $26 million to resolve a *qui tam* lawsuit alleging Stark law violations for allegedly overcompensating referring physicians, as well as a self-disclosure related to false meaningful use attestations (discussed more below).[50]
- Also, in December 2017, Pine Creek Medical Center, a physician-owned hospital in Dallas, Texas, agreed to pay $7.5 million to resolve an FCA *qui tam* suit alleging payment of kickbacks in the form of marketing services to physicians in exchange for surgical referrals. According to the DOJ, the remuneration included the hospital paying for advertisements on behalf of the physicians in local and regional publications, as well as radio and television advertising, pay-per-click advertising campaigns, billboards, Web site upgrades, and business cards.[51]

These settlements and others make clear that the government remains committed to investigating and punishing alleged violations of the Stark law and the AKS.

Compounding Fraud

Although overtaken in 2017 by opioid fraud and abuse enforcement, government enforcement in the compounding pharmacy space hit an all-time high in the last several years. Typically, these investigations involve alleged kickback schemes between pharmacies and their sales representatives, on the one hand, and prescribing physicians, on the other. The government's enforcement activities picked up tremendously in 2015, when various news organizations began to report soaring prices that Tricare paid to compounding pharmacies. For example, in November 2015, the *Wall Street Journal* reported that compounding pharmacies often charged Tricare between $10,000 and $40,000 for a one-month supply of compounded medication, typically pain and/or scar cream.[52]

According to that same article, Tricare's spending on compounded drugs skyrocketed from $500 million in FY 2014 to $1.75 billion in FY 2015. Much of the fraud involving compounding pharmacies, according to the Journal, was due in part to the fact that sales representatives for the compounding pharmacies typically got paid on a commission basis, thereby giving them the financial incentive to pay kickbacks to prescribing physicians in order to encourage more prescriptions. Some examples of enforcement activities in the compounding pharmacy space include:

- In February 2018, the DOJ announced that it had intervened in an FCA *qui tam* filed against Patient Care America, a Florida-based compounding pharmacy. According to the government's press release, the pharmacy paid illegal kickbacks to induce prescriptions for compounded drugs reimbursed by Tricare. Also named in the suit were two of the pharmacy's executives and a private equity firm that managed the pharmacy.[53]
- The following month, the DOJ announced that the owner of an Alabama-based compounding pharmacy had been sentenced to five years in federal prison for conspiring to defraud a federal health care program out of more than $10 million. According to the government, the defendant paid kickbacks to independent sales representatives as an incentive to refer Tricare prescriptions, sold misbranded over-the-counter medications as prescription drugs, and failed to reverse claims on prescriptions that he knew were forged.[54]
- In April 2018, the owner of several Florida-based compounding pharmacies was sentenced to 15 years in federal prison and ordered to pay more than $50 million in restitution for his role in an illegal scheme to defraud Tricare. According to the government, the defendant manipulated billing codes and submitted reimbursement claims for pharmaceutical ingredients that they did not have. The defendant also paid kickbacks and bribes to patients and physicians in exchange for prescriptions.[55]

Although prosecutions related to compounding pharmacies have slowed a bit while the government focuses on other areas of fraud and abuse, including those related to opioids, all indications are that compounding pharmacies and their owners and sales representatives will continue to remain a focus for federal authorities into the future.

Reading the Tea Leaves: What's Next?

EHR-Related Fraud and Abuse

As the health care industry, and providers in particular, become more reliant on electronic health records (EHRs) and related technology, federal regulators are sure to focus more of their resources on potential EHR-related fraud and abuse. This is, in fact, a trend that has already started. As discussed briefly above, in December 2017, 21st Century Oncology paid $26 million to resolve a government investigation revolving around, among other things, a self-disclosure involving the submission of false

attestations to CMS concerning employed physicians' use of EHR software.[56] The self-disclosure included admissions that company employees falsified data regarding the company's use of EHR software, fabricated utilization reports, and superimposed EHR vendor logos onto the reports to make them look legitimate.[57]

Earlier that year, in May 2017, eClinicalWorks (ECW)—one of the nation's leading EHR software vendors—agreed to pay $155 million to resolve an FCA *qui tam* which alleged that it misrepresented the capabilities of its software and paid kickbacks to certain customers in exchange for promoting its product.[58] According to the DOJ, ECW falsely obtained meaningful use certification from the government by concealing certain information from the certifying entity.[59] The next month, in June 2017, the OIG issued a report stating that Medicare had paid nearly $730 million in EHR incentive payments that did not comply with federal regulations.[60] Several weeks after releasing this report, the OIG updated its work plan to include a review of incentive payments made to health care providers for adopting EHR technology.[61]

While health care providers are familiar with meaningful use of incentive payment audits by Medicare, Medicaid, and its contractors, moving forward, providers should expect an increase in DOJ- and OIG-led fraud and abuse investigations involving allegations of false meaningful use attestations.

Telehealth

As is the case in many industries, the pace of technological innovation in health care has greatly outpaced changes in health care laws and regulations. There is perhaps no better example of this phenomenon than in telehealth. While telehealth technologies are improving on an almost-daily basis, CMS' telehealth regulations remain stagnant. Specifically, in order for telehealth services to be reimbursable by Medicare, the beneficiary has to be at a qualifying "originating site," the technology used has to meet very specific requirements, the services must be performed by an eligible practitioner, and, even when all of these requirements are satisfied, still only certain services are covered.[62]

The combination of rapidly expanding technology and rigid regulations are sure to see an increase in fraud and abuse enforcement related to telehealth services. Although there are very few reported enforcement actions related to telehealth,[63] all indications are that such actions will increase in the foreseeable future. In October 2017, for example, the OIG supplemented its work plan to announce that it will audit Medicare claims paid for telehealth services to ensure compliance with CMS' requirements.[64] In April 2018, the OIG released a report that nearly one-third of the telehealth claims that it reviewed did not meet CMS' telehealth requirements.[65] Based on these findings, the OIG recommended that CMS conduct periodic post-payment reviews for telehealth services and offer education and training sessions for providers.[66] The OIG's findings all but guarantee that federal regulators will continue to focus on potentially improper telehealth payments, and thus providers should be prepared for an increase in fraud and abuse enforcement in this area.

Conclusion

The federal government's continued annual billion-dollar recoveries in health care fraud and abuse enforcement will ensure that health care providers remain the target of government enforcement for years to come. While new areas continue to pop up on the government's enforcement radar—including, most recently, opioid fraud and abuse, compounding pharmacy fraud, and telehealth abuse—there are some enforcement staples that will continue steadily into the future, including enforcement under the Stark law and the AKS. Health care providers should remain vigilant and proactive to avoid finding

themselves on the receiving end of a costly and lengthy government investigation.

Endnotes

1. DOJ Fraud Statistics—Health and Human Services, available at www.justice.gov/opa/press-release/file/1020116/download.
2. *Id.*
3. 31 U.S.C. § 3730(d).
4. DOJ Fraud Statistics.
5. It is important to note that many states have their own versions of the False Claims Act. For example, the State of Georgia has two state FCAs—the Taxpayer Protection False Claims Act (O.C.G.A. § 23-3-120 *et seq.*) and the State False Medicaid Claims Act (O.C.G.A. § 49-4-168 *et seq.*). This article will focus exclusively on the federal FCA.
6. 31 U.S.C. § 3730.
7. DOJ Press Release Dated December 21, 2017, available at www.justice.gov/opa/pr/justice-department-recovers-over-37-billion-false-claims-act-cases-fiscal-year-2017.
8. CMS, 2016-2025 Projections of National Health Expenditures Data Released, available at www.cms.gov/Newsroom/MediaReleaseDatabase/Press-releases/2017-Press-releases-items/2017-02-15-2.html.
9. 31 U.S.C. § 3729(b)(4).
10. 31 U.S.C. § 3729(b)(1).
11. *Id.*
12. 31 U.S.C. § 3729(a)(1)(G).
13. CMS, *Medicare Reporting and Returning of Self-Identified Overpayments*, available at www.cms.gov/Newsroom/MediaReleaseDatabase/Fact-sheets/2016-Fact-sheets-items/2016-02-11.html.
14. 31 U.S.C. § 3729. Note that per-claim penalties have been adjusted for inflation.
15. 42 U.S.C. § 1320a-7.
16. Like the FCA, various states have their own version of the Stark law, often referred to as "Baby Stark" laws. This article focuses exclusively on the federal Stark law.
17. 42 U.S.C. § 1395nn.
18. *Id.*
19. 42 C.F.R. § 411.351. Providers can access a database with procedure codes that qualify as DHS through CMS Web site at www.cms.gov/Medicare/Fraud-and-Abuse/PhysicianSelfReferral/List_of_Codes.html.
20. 42 C.F.R. § 411.354(a).
21. Stark defines an "immediate family member" to include a spouse, parent, child, sibling, stepparent, stepchild, stepsibling, parent-in-law, child-in-law, grandparent, grandchild, and spouse of a grandparent or a grandchild. *Id.* at § 411.351.
22. *Id.* at 411.353(c).
23. *Id.* at 411.351.
24. 42 C.F.R. § 411.357(a) and (b).
25. *Id.* at 411.357(c).
26. *Id.* at 411.357(d).
27. 42 U.S.C. § 1320a-7a.
28. See, e.g., *U.S. ex rel. Parikh v. Citizens Medical Center*, 977 F. Supp. 2d 654, 672 (S.D. Tex. 2013).
29. Numerous states also have their own versions of the anti-kickback statute. This article will focus exclusively on the federal statute.
30. 42 U.S.C. § 1320a-7b(b).
31. *Id.*
32. These penalties were increased as part of the Bipartisan Budget Act of 2018.
33. 42 U.S.C. § 1320a-7a.
34. 42 U.S.C. § 1320a-7b(g).
35. *Id.* at 1320a-7b(h).
36. 42 C.F.R. § 1001.952.
37. www.justice.gov/opa/pr/national-health-care-fraud-takedown-results-charges-against-over-412-individuals-responsible.
38. *Id.*
39. www.justice.gov/opa/pr/attorney-general-sessions-announces-opioid-fraud-and-abuse-detection-unit.
40. *Id.*
41. *Id.*
42. www.justice.gov/opa/pr/attorney-general-sessions-announces-dea-surge-combat-prescription-drug-diversion.
43. www.justice.gov/opa/pr/dea-surge-drug-diversion-investigations-leads-28-arrests-and-147-revoked-registrations.
44. *Id.*
45. www.justice.gov/opa/pr/attorney-general-sessions-announces-new-prescription-interdiction-litigation-task-force.
46. *Id.*
47. *Id.*
48. www.justice.gov/opa/pr/los-angeles-hospital-agrees-pay-42-million-settle-alleged-false-claims-act-violations-arising.
49. www.justice.gov/opa/pr/new-york-hospital-operator-agrees-pay-4-million-settle-alleged-false-claims-act-violations.
50. www.justice.gov/opa/pr/21st-century-oncology-pay-26-million-settle-false-claims-act-allegations.
51. www.justice.gov/opa/pr/dallas-based-physician-owned-hospital-pay-75-million-settle-allegations-paying-kickbacks.
52. www.wsj.com/articles/u-s-targets-pharmacies-over-soaring-claims-to-military-health-program-1447032619.
53. www.justice.gov/opa/pr/united-states-files-false-claims-act-complaint-against-compounding-pharmacy-private-equity.
54. www.justice.gov/usao-ndal/pr/compounding-pharmacy-owner-sentenced-five-years-prison-105-million-health-care-fraud.
55. www.justice.gov/opa/pr/owner-florida-pharmacy-sentenced-15-years-prison-100-million-compounding-pharmacy-fraud.
56. www.justice.gov/opa/pr/21st-century-oncology-pay-26-million-settle-false-claims-act-allegations.
57. *Id.*

58. www.justice.gov/opa/pr/electronic-health-records-vendor-pay-155-million-settle-false-claims-act-allegations.
59. *Id.*
60. oig.hhs.gov/oas/reports/region5/51400047.asp.
61. oig.hhs.gov/reports-and-publications/archives/workplan/2017/hhs%20oig%20work%20plan%202017.pdf.
62. www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNProducts/downloads/telehealthsrvcsfctsht.pdf.
63. In July 2016, a Connecticut physician and practice group agreed to pay $36,000 in the first-reported FCA matter related to telehealth. The *qui tam* complaint in that case alleged that the group billed Medicare for services provided over the telephone that did not qualify for telehealth payments. www.justice.gov/usao-ct/pr/danbury-physician-and-mental-health-practice-pay-36000-settle-false-claims-act. In February 2018, the DOJ filed a *qui tam* complaint against Patient Care America compounding pharmacy (discussed briefly above). Part of the allegations in that case was that the pharmacy submitted claims to Medicare for services that amounted to non-reimbursable telehealth services. www.justice.gov/opa/pr/united-states-files-false-claims-act-complaint-against-compounding-pharmacy-private-equity.
64. www.oig.hhs.gov/reports-and-publications/workplan/summary/wp-summary-0000259.asp.
65. oig.hhs.gov/oas/reports/region5/51600058.asp.
66. *Id.*

Reprinted from Journal of Health Care Compliance, Volume 20, Number 4, July–August 2018, pages 5–12, 63 with permission from CCH and Wolters Kluwer.
For permission to reprint, e-mail permissions@cch.com.