Fraud and Compliance Considerations for Telemedicine and Digital Health: Navigating the Emerging Landscape

Erica Kraus, Sheppard Mullin
Ty Kayam, Microsoft

Introduction and Trends

a. Leveraging Technology to Combat Fraud: In 2009, the DOJ and HHS-OIG established the Health Care Fraud Prevention and Enforcement Action Team (HEAT) to build and strengthen existing programs combating Medicare fraud, while investing new resources and technology to prevent and detect fraud and abuse. Tools and technologies used for this purpose include AI tools to analyze proper billing for reimbursable services and data mining and matching to analyze billing and beneficiary utilization practices to identify potential fraudulent activity.

b. Role of Technology in Shifting Toward Value-Based Care: HHS launched its Regulatory Sprint to Coordinated Care, intended to address provider concerns about regulatory impediments to arrangements that would promote quality and efficiency and accelerate the transformation of the health care system toward value-based payment. This HHS effort both recognizes and begins to accommodate an industry-wide shift toward value-based care, which requires new mechanisms and partnerships to leverage technological solutions.

c. Opportunities and Enforcement Related to COVID-19: The COVID-19 pandemic accelerated adoption of technologies including telehealth platforms and remote patient monitoring devices that allowed patients to receive more care from their homes. In response to the unique challenges the pandemic posed for the health care system, HHS also released a variety of waivers relieving providers from compliance with certain regulatory requirements. These changes allowed for innovative solutions and partnerships during the pandemic, but have also laid the groundwork for heightened post-pandemic enforcement. DOJ, CMS, and HHS-OIG are working to investigate and address new risks and schemes stemming from the waivers and flexibilities during the COVID-19 pandemic, including health care technology schemes. These include false and fraudulent representations about COVID-19 testing, treatments, or cures that are used to defraud insurance carriers, patients, and business investors. In addition, there is focus on fraudulently obtained COVID-19 health care relief funds under the Coronavirus Aid, Relief, and Economic Security (CARES) Act's Provider Relief Fund, the Paycheck Protection Program and Health Care Enhancement Act, or the Economic Impact Disaster Loan (EIDL) program. *See* FY2020 Health Care Fraud and Abuse Control Program Annual Report (hhs.gov).

Relevant Fraud and Abuse Laws

A. The Anti-Kickback Statute

1. The Anti-Kickback Statute ("AKS") makes it a felony to knowingly exchange remuneration to induce the referral, recommendation, or arrangement of business

reimbursable by the Federal health care programs. *See* 42 U.S.C. § 1320a-7b. Violations of the AKS may also be a basis for civil False Claims Act liability.

2. The AKS applies to companies that provide items or services reimbursable by the Federal health care programs whether or not those companies themselves submit claims to the Federal health care programs. If a company sells items or services to a customer and the customer claims Federal health care program payment, whether on a fee-for-service basis, via cost reporting, or otherwise, the seller company may be subject to the AKS. Technology companies that provide items or services to health care providers and suppliers should be mindful of AKS restrictions.

3. There are both statutory exceptions and regulatory safe harbors describing conduct that is not subject to AKS liability. Compliance with all of the requirements of an exception or safe harbor immunizes conduct from liability. Failure to comply with all the requirements of an exception or safe harbor does not make conduct illegal, but requires a case-by-case analysis of risk.

4. In November 2020, the OIG released rules creating new safe harbors for participants in value-based arrangements and for certain cybersecurity donations, and clarifying an existing safe harbor for EHR donations. These changes create new opportunities for technology companies and health care providers, among others, to protect arrangements from AKS liability.

5. Key Exceptions to Consider for Telemedicine and Digital Health Arrangements:

    a. Value-Based Arrangements. Four new safe harbors may protect remuneration exchanged by participants in a “”value-based enterprise.” These participants may be health care providers, technology companies, management organizations, or others, although limitations apply to the protection available to certain health care industry participants, including pharmaceutical companies, laboratories, compounding pharmacies, PBMs, DME manufacturers and suppliers, and medical device manufacturers and distributors. Safe harbors applicable to financial remuneration require the VBE to accept risk, but others applicable to in-kind remuneration are less demanding. *See* 42 C.F.R. § 1001.952(ee)-(hh).

    b. Investments in Small Entities. The safe harbors for value-based arrangements are explicitly unavailable to protect ownership interests. Companies seeking to offer ownership interests to potential business referral sources should consider the applicability of the safe harbor for investments in small entities. *See* 42 C.F.R. § 1001.952(a)(2).

    c. Personal Services Safe Harbor. Offering protection to arrangements for personal services, this safe harbor was recently amended to apply to arrangements where aggregate compensation is not set in advance, provided that the methodology for determining compensation is set in advance and not determined in a manner that

takes into account the volume of business generated between the parties, and that the arrangements meets other safe harbor criteria. The safe harbor now also provides explicit protection for certain outcomes-based payment arrangements. *See* 42 C.F.R. § 1001.952(d).

d. Warranties and Discounts. These safe harbors protect warranties and discounts meeting certain criteria. *See* 42 C.F.R. § 1001.952(g), (h). Companies in or working with partners in the health care space should consider implementing contracting policies requiring compliance with these safe harbors.

e. Group Purchasing Organizations. This safe harbor offers protection for fees paid to GPOs; compliance should be considered whenever a company is entering into a GPO arrangement. *See* 42 C.F.R. § 1001.952(j).

f. Managed Care. These safe harbors offer broad protection for many arrangements between managed care entities and their first tier and downstream contractors to provide or arrange for items or services to managed care patients. *See* 42 C.F.R. § 1001.952(t), (u).

g. Electronic Prescribing Items and Services. This safe harbor protects certain donations of technology used to transmit and receive electronic prescription information. *See* 42 C.F.R. § 1001.952(x).

h. Cybersecurity Technology and Services. A new safe harbor for certain donations of cybersecurity technology and services under specific conditions. *See* 42 C.F.R. § 1001.952(jj).

i. Electronic Health Records Items and Services. This safe harbor protects certain donations of EHR items and services to eligible recipients under specific conditions. *See* 42 C.F.R. § 1001.952(y). Recent modifications to the existing safe harbor add protections for certain related cybersecurity technology, update provisions regarding interoperability, and remove the sunset date.

B. The False Claims Act

1. The False Claims Act ("FCA"), 31 U.S.C. § 3729, prohibits the knowing submission of false claims to the government, as well as the use of records material to false claims, and the knowing retention of overpayments. A claim may be either factually false or may be false by virtue of non-compliance with a law or regulation to which a claimant has expressly or impliedly certified compliance. The FCA also creates liability for *causing* a violation of these prohibitions, such that it may apply not only to entities that submit claims to the government, but also to those that engage in business with claimants.

2. In 2020, the Justice Department recovered over $2.2 billion in FCA cases, with over $1.8 billion related to matters involving the health care industry. Telemedicine and technology companies are increasingly targets of FCA actions. For instance,

Operation Rubber Stamp (discussed further below) identified more than $1.5 billion of fraudulent billings related to a telemedicine scheme in which clinicians were allegedly paid to order DME, labs, or pharmaceuticals without adequate medical evaluation of patients, and which orders were sold to DME suppliers, laboratories, and pharmacies. A series of investigations - discussed further below - has targeted EHR vendors, and has resulted in several substantial settlements.

C. *Stark Law*

1. The Stark Law prohibits physicians from referring certain designated health services to entities with which they have unexpected financial relationships. *See* 42 U.S.C. § 1395nn.

2. The Stark Law impacts the appropriate structure of financial relationships between physicians and entities - like hospitals, laboratories, imaging centers, and DME suppliers - that furnish designated health services, and therefore the ability of such entities to share technology and technology support with physicians.

3. New exceptions to the Stark Law protect certain remuneration exchanged under a "value-based arrangement." *See* 42 C.F.R. § 411.357(aa). These exceptions may offer significant flexibility to entities to pay physicians for their engagement with value-based activities, or to provide various technology and technological support to physicians to support participation in value-based activities.

4. Other exceptions may protect particular types of technology donations. For instance, exceptions exist for IT information and services that enable participation in a community-wide information system, certain electronic prescribing items and services, certain EHR items and services, and certain cybersecurity technology and related services. *See* 42 C.F.R. § 411.357(u), (v), (w), (bb).

5. Each of these exceptions is limited to compensation arrangements - exceptions available for ownership interests are much more limited.

D. *Civil Monetary Penalties*

1. The Civil Monetary Penalties Law ("CMPL") allows the OIG to sanction certain conduct, including the offer or transfer of remuneration to a Medicare or Medicaid beneficiary that the offerer knows or should know is likely to influence the beneficiary to order or receive items or services payable by a Federal health care program from a particular provider, practitioner, or supplier. *See* 42 U.S.C. § 1320a-7a(a)(5). Provision of technology items or services to patients may implicate the CMPL if such provision is likely to influence the patient to select a particular provider for new or continuing treatment.

2. The law provides for certain exceptions to the definition of "remuneration." Provision of technology items and services that fits within one of these exceptions will not result in liability under the CMPL. *See* 42 U.S.C. § 1320a-7a(i)(6); *See* 42 C.F.R. § 1003.110.

Among these exceptions, the following may be most relevant to transfers of technology items and services:

a. Incentives given to individuals to promote the delivery of preventive care. This exception protects certain reasonable incentives for patients to receive a defined set of preventive services. For instance, this exception might protect provision to patients by a provider of an app that tracks their receipt of defined medically appropriate preventive care services, and allows them to receive reward points for such receipt that are exchangeable for limited value non-cash items.

b. Remuneration that promotes access to care and poses a low risk of harm to patients and the FHCPs. To fit within this exception, remuneration should remove an obstacle to a patient's ability to access health care items and services payable by the FHCPs. For instance, an app that helps manage appointment scheduling and arrange transport to appointments or enables communication with health care providers for homebound patients could potentially fit within this exception.

c. Items and services reasonably connected to the medical care of an individual who is in financial need, if the items or services are not advertised or tied to the provision of other federally reimbursable items and services. This exception could protect the provision of medical equipment or technological software or supports for use of equipment or to promote adherence to a care plan. For instance, under some circumstances, this exception could protect the provision of smart phones to low-income patients to enable the transmission of data from a medical device to the patient's health care providers.

d. Telehealth technologies for in-home dialysis. A recent amendment to the CMPL definition of "remuneration" in the CMP rules protects "telehealth technologies" furnished by certain providers to ESRD patients receiving in-home dialysis under certain conditions.

E. *State Analogs*

1. Many states have their own anti-kickback, false claims, and anti-self-referral laws.

2. These laws may be broader, narrower, or simply different in scope than the federal laws above. Consider applicable state laws before concluding that any proposed arrangement is permissible.

F. *Other State Law Considerations*

1. Fee-splitting - Many states disallow professionals from splitting fees from their professional services with others, especially where such split may influence referrals or professional judgment. These prohibitions may limit permissible financial arrangements between doctors or professional entities and others. For instance, payment of a

percentage of professional fee collections to a telehealth platform provider for each visit furnished via the platform could potentially implicate certain fee-splitting prohibitions.

2. Corporate Practice of Medicine - Many states have rules against the engagement in clinical activities by non-professional persons and entities. Some of these rules may not allow non-professional entities, including many management services organizations or other vendors, to employ or contract with licensed clinicians or to make or influence decisions that impact clinical practice. These rules may affect the scope of work that may be undertaken by non-professional technology companies, and the way in which relationships between these companies and professionals must be structured.

3. Licensure - Most states require that doctors and other clinicians furnishing professional services to patients within their borders be licensed in the state. As a result, a physician licensed in one state may not be allowed to furnish medical services to patients sitting in another state, including via telehealth. Many states have loosened or waived licensure requirements during the COVID-19 pandemic, but these relaxations are being rolled back.

Applicability of Fraud and Abuse Laws

A. By Activity

1. Telehealth and Telemedicine

   a. During the COVID-19 pandemic, the use of telehealth and telemedicine (collectively, "telehealth") tools and solutions has accelerated in part due to necessity and also due to temporary waivers and flexibilities under the Public Health Emergency. For instance - and critically - CMS waived statutory restrictions on the locations where Medicare will cover telehealth services to allow patients to receive telehealth services from their homes. CMS also expanded its list of services that may be covered via telehealth, and offered additional flexibility as related to smartphone use and supervision requirements. CMS has taken steps to extend some of these flexibilities beyond the pandemic, although the statutory location restriction may remain in place absent Congressional intervention.

   b. While OIG has taken various enforcement actions related to telehealth fraud and abuse, an uptick in enforcement can be expected:

      i. While "OIG recognizes the promise that telehealth and other digital health technologies have for improving care coordination and health outcomes", it is also "conducting significant oversight work assessing telehealth services during the public health emergency." *See* HHS-OIG Principal Deputy Inspector General Grimm on Telehealth.

ii. OIG is currently conducting *eight* reviews related to the use of telehealth services. *See* *Work Plan | Office of Inspector General | U.S. Department of Health and Human Services (hhs.gov)*.

c. Many of the OIG audits focus on compliance with Medicare and Medicaid requirements for documenting and billing home health services. These audits are, in a sense, traditional billing and coding audits applied to telehealth services, although challenges may arise in interpreting the scope of the various regulatory flexibilities that applied during the COVID-19 pandemic. Enforcement may also focus on fraud and anti-kickback allegations, as were pursued in Operation Rubber Stamp (discussed below). Risk could also be associated with the telehealth platform and technology providers, as well as technology donations and price reductions to physicians and to patients.

d. Other Policy Changes during the COVID-19 Pandemic:

i. In response to the COVID-19 pandemic, OIG issued a policy statement to notify physicians and other practitioners that they will not be subject to administrative sanctions for reducing or waiving any cost sharing obligations that beneficiaries of federal health care programs may owe for telehealth services furnished consistent with applicable coverage and payment rules, subject to certain conditions. *See* *OIG Policy Statement (hhs.gov)*. OIG has supplemented this announcement with a FAQ noting that this policy statement applies to "a broad category of nonface-to-face services furnished through various modalities, including telehealth visits, virtual check-in services, e-visits, monthly remote care management, and monthly remote patient monitoring." *See* *FAQ--Telehealth Services Policy Statement (hhs.gov)*.

ii. CMS issued guidance that Medicare Advantage Organizations (MAOs) may provide enrollees with access to Medicare Part B services via telehealth in any geographic area and various locations, including the beneficiaries' homes. CMS further exercised their enforcement discretion related to MAOs expanding coverage of telehealth services beyond those approved by CMS in the plan's benefit package for similarly situated enrollees impacted by the outbreak, as approved by CMS, until it is determined that the exercise of this discretion is no longer necessary in conjunction with the COVID-19 outbreak. CMS confirmed with HHS OIG that such additional coverage would satisfy the safe harbor to the Federal anti-kickback statute set forth at 42 CFR 1001.952(l). *See* *COVID-19 Updated Guidance for MA and Part D Plan Sponsors 5.22.20 (cms.gov)*.

e. OIG Advisory Opinions Related to Telehealth:

i. OIG Advisory Opinion No. 18-03: The OIG concluded that it would not impose administrative sanctions on a federally qualified health center

look-alike's proposal to provide information technology items and services, without charge, to a county Department of Health's clinic to facilitate telemedicine encounters. In concluding that the proposal posed a low risk of fraud and abuse, the OIG considered several factors: (1) the clinic would be free to refer to other providers, patients would remain free to choose other providers, and the technology would not be limited to use with the FQHC look-alike, (2) there would be no steering toward the FQHC look-alike's pharmacy, (3) the arrangement would be unlikely to increase costs to the Federal health care programs, and could potentially decrease them through better access to preventative services, and (4) the primary beneficiaries of the proposed arrangement would be clinic patients.

ii. OIG Advisory Opinion No. 11-12: The OIG concluded that it would not impose administrative sanctions on a health system's proposal to enter into arrangements to provide neuro emergency clinical protocols and neuro emergency telemedicine technology and immediate consultations with stroke neurologists via telemedicine technology to certain community hospitals. In concluding that the proposal posed a low risk of fraud and abuse, the OIG considered several factors: (1) the health system would be unlikely to generate appreciable referrals through the arrangement, and in fact might decrease transfers of stroke patients, (2) participation would initially be offered only to affiliated hospitals, and participation would never be conditioned on the volume or value of referrals, (3) the primary beneficiaries of the arrangement would be stroke patients, (4) there would be no requirement to engage in marketing activities and no party would fund marketing activities for another, and (5) the arrangement would be unlikely to increase costs to the Federal health care programs, as consultations would not generally be billable and the goal of the program would be to reduce the volume of stroke patient transfers.

iii. OIG Advisory Opinion No. 98-18: The OIG concluded that it would not sanction an ophthalmologist's proposed sublease to an optometrist of certain imaging equipment to enable the ophthalmologist to perform telemedicine consultations on the optometrists patients because (1) the sublease would meet the criteria of the equipment rental safe harbor, 42 C.F.R. § 1001.952(c), and (2) there was low risk of fraud or abuse associated with the provision of consultations. With respect to its conclusion on the provision of consultations, the OIG noted that the optometrist would not advertise or market her access to the consultations or charge a fee for the consultations, such that they would have minimal, if any, value to the optometrist. Further, the arrangement provided the optometrist's patients freedom to choose any ophthalmologist and the parties certified that there was no arrangement between them with respect to referrals, such that the opportunity for the ophthalmologist to

generate business from the consultations would not induce the ophthalmologist to refer business to the optometrist.

c. Examples of Enforcement:

- Operation Rubber Stamp: In October 2020, DOJ announced a historic nationwide enforcement action involving 345 charged defendants across 51 federal districts, including more than 100 doctors, nurses, and other licensed medical professionals. The largest amount of alleged fraud loss charged in connection with those cases related to schemes involving telemedicine. In addition to the criminal charges announced related to the enforcement action, CMS' Center for Program Integrity (CPI) separately announced that it has taken a record-breaking number of administrative actions related to telemedicine fraud, revoking the Medicare billing privileges of 256 additional medical professionals for their involvement in telemedicine schemes. This represents the largest number of adverse administrative actions resulting from a single administrative health care fraud investigative initiative. *See Operation Rubber Stamp: Major health care fraud investigation results in significant new charges | USAO-SDGA | Department of Justice*.

- Operation Brace Yourself: In April 2019, the DOJ, HHS OIG, and the FBI announced charges against 24 defendants for their alleged participation in health care fraud schemes involving the payment of illegal kickbacks and bribes by DME companies in exchange for the referral of Medicare beneficiaries by medical professionals working with fraudulent telemedicine companies for back, shoulder, wrist and knee braces that are medically unnecessary. See Federal Indictments & Law Enforcement Actions in One of the Largest Health Care Fraud Schemes Involving Telemedicine and Durable Medical Equipment Marketing Executives Results in Charges Against 24 Individuals Responsible for Over $1.2 Billion in Losses | OPA | Department of Justice

2. Donating Technology

a. Many circumstances may arise where one entity wishes to donate technology to another for a variety of reasons. Sometimes, such technology may be fundamentally and integrally related to the donor's items and services, and provide only "incidental" value to the recipient. In these cases, a donation might not constitute remuneration at all, and therefore may not implicate the AKS or the Stark Law.

- For instance, OIG guidance has noted approval of arrangements wherein a laboratory provides a computer to a physician office *if* the computer's utility is wholly limited to receiving and reviewing laboratory test results.

- Similarly, in OIG Advisory Opinion No. 12-20, the OIG concluded that it would not impose administrative sanctions on a hospital's proposed arrangements to provide free access to an electronic interface to community physicians and physician practices that would allow those physicians and practices to transmit orders for certain services to, and receive the results of those services from, the hospital. The OIG concluded that such access would not constitute remuneration to the physicians since "access would be integrally related to the Requestor's services, such that free access would have no independent value to the Physicians apart from the services that Requestor provides."

b. In other cases, donated technology may confer independent value on the recipient. Some such donations may nevertheless be protected because they fall within applicable AKS safe harbors and Stark Law exceptions. As discussed above, AKS safe harbors and Stark Law exceptions are available for certain donations of electronic prescribing, EHR, and cybersecurity items and services.

c. In still other cases, a donation might confer remuneration to a recipient and also fall outside AKS safe harbors, but nevertheless not violate the AKS because it was not made with an intent to induce the recipient's arrangement of business for the donor. Such donations would need to be considered on a case-by-case basis and would need to incorporate appropriate safeguards.

B. By Entity or Interaction with Entity

1. <u>Hospitals, Clinicians, and Other Providers</u>

a. Clinical health care providers seeking to furnish and bill for services including or provided via new technologies must be familiar with applicable billing and coding requirements. Claims for health care services are processed based on standardized code sets that identify services furnished to patients. While still evolving, CMS has begun establishing various codes and mechanisms for the reimbursement of digital health and other technologies. Some examples include the introduction of CPT code 9225X as part of the 2021 Physician Fee Schedule for the use of autonomous artificial intelligence in a primary care setting to detect diabetic retinopathy and the proposed Medicare Coverage for Innovative Technology (MCIT) coverage pathway to allow Medicare reimbursement of breakthrough devices that obtain FDA authorization. Similar to other services covered by Medicare, organizations must ensure that any submission of claims to a Federal health care program for these emerging technologies are provided as claimed, correctly billed, and "reasonable and necessary" in accordance with section 1862(a)(1)(A) of the Social Security Act. Similarly, telehealth is subject to particular and evolving coding and billing requirements, some of which are distinct to telehealth furnished during the current PHE. CMS has also clarified coverage requirements for remote patient monitoring codes. For instance, CMS clarified that the twenty minutes of time required to bill 99457 and 99458 could

include both real-time communications and other care management services. CMS has also clarified that 99453 and 99454 can be reported only once per patient per thirty day period, and can be reported by only one practitioner for a patient.

b. Clinical providers may also choose to partner with technology companies offering devices, platforms, or similar items and services that may enhance patient care, particularly as reimbursement shifts to emphasize quality, efficiency, and coordination. In structuring these relationships, providers should be cognizant of restrictions imposed by the AKS and other fraud and abuse laws (discussed above). Parties should consider opportunities to avail themselves of the new value-based safe harbors described above.

2. *Medical Device Manufacturers*

a. Over the past few decades, the Food and Drug Administration ("FDA") has played an integral role in the area of digital health. The FDA has oversight over medical devices, including software as a medical device ("SaMD") and software in a medical device ("SiMD"). Medical devices are eligible for reimbursement by CMS if they are within a category of product or service covered by Medicare (as specified in the Social Security Act) and are "reasonable and necessary" for a patient's treatment. *See* 42 U.S.C. 1395y(a)(1)(A). Although in many cases, SaMD and SiMD may not be directly reimbursable by the Federal health care programs, their costs may nevertheless be indirectly passed onto the programs via cost reporting or other mechanisms, or payments for a device containing SiMD may be integrally connected to purchases of the SiMD, which relationships could put SaMD and SiMD developers within the ambit of the AKS and other fraud and abuse laws.

b. Manufacturers of medical devices could trigger fraud and abuse laws through marketing or other promotional practices related to the device or through financial relationships that result in prohibited remuneration or kickbacks, such as excessive fees to physicians for speaking at engagements or for consulting arrangements, royalties on devices, extravagant gifts to physicians or their family members, or paying physicians for obtaining new customers. *See* Medical Device Law and Regulation Answer Book - 2021 Edition, S. Onel and K. Becker. Both providers and medical device manufacturers may be held liable for knowingly violating fraud and abuse laws. In some cases, medical device manufacturers may have a critical role to play in arrangements to improve care coordination for patients, including through donations, data-sharing, provider partnerships, and other mechanisms. However, given enforcement focus on this sector - and device manufacturer exclusion from some of the protections available to other entity types under the new value-based safe harbor - parties should be especially careful in structuring arrangements between medical device manufacturers and others.

c. Examples of Enforcement:

i. NuVasive, Inc.: NuVasive agreed to pay $13.5 million to resolve allegations that the company promoted its CoRoent System for surgical uses that were not approved or cleared by FDA, caused physicians to submit claims for Medicare and Medicaid reimbursement that were not eligible for reimbursement, and paid kickbacks and other remuneration to induce physicians to use its CoRoent System, including promotional speaker fees, honoraria, and expenses for event attendance. *See* Medical Device Manufacturer NuVasive Inc. to Pay $13.5 Million to Settle False Claims Act Allegations | OPA | Department of Justice.

ii. Sanford Health: Sanford Health, Sanford Medical Center, and Sanford Clinic (collectively, "Sanford") agreed to pay $20.3 million to resolve civil FCA allegations that Sanford knowingly submitted false claims to federal health care programs resulting from violations of the AKS and medically unnecessary spinal surgeries. The government alleged that Sanford knew that one of its top neurosurgeons was improperly receiving kickbacks from his use of implantable devices distributed by his physician-owned distributorship, but continued to employ the neurosurgeon, continued to allow him to profit from the devices he used in surgeries performed at Sanford, and continued to submit claims to federal health care programs for these surgeries, including for procedures that were medically unnecessary. *See* "The Department of Health and Human Services and Justice Health Care Fraud and Abuse Control Program Annual Report for Fiscal Year 2020," July 2021, at 23.

iii. Covidien LP: Covidien agreed to pay $13 million to resolve civil FCA allegations that it paid kickbacks to induce the use of its Solitaire mechanical thrombectomy device. Covidien launched a registry to pay hospitals and institutions to collect data about user experiences with the device and paid a fee to hospitals and institutions that participated in the registry each time they used a new Solitaire device and reported certain clinical data about their practices. Certain hospitals and institutions were solicited for the registry in order to convert their business from the competitor's product and/or persuade them to continue using Covidien products. *See* "The Department of HEalth and Human Services and Justice Health Care Fraud and Abuse Control Program Annual Report for Fiscal Year 2019," June 2020, at 18.

3. Electronic Health Record (EHR) Systems and Certified Health IT

a. In 2010, as part of implementing provisions within the American Recovery and Reinvestment Act of 2009, CMS created the Medicare and Medicaid EHR Incentive Programs whereby eligible professionals (EPs), eligible hospitals (EHs), and critical access hospitals (CAHs) that were "meaningful users" of

certified EHR technology would receive incentives under either the Medicare or Medicaid incentive programs. The Office of the National Coordinator for Health IT (ONC) created a complementary certification program for developers of EHRs or other health IT providers (namely, developers of health IT modules or "relied-upon" software). EPs, EHs, and CAHs were required to attest that they were using certified electronic health record technology (CEHRT) that was certified by ONC. To be certified, developers had to meet the applicable edition of the certification criteria and undergo review, testing, and surveillance. The EHR Incentive Programs have now been renamed the Promoting Interoperability programs, and some portions have been discontinued and replaced with the Quality Payment Program. Nonetheless, the requirement for providers to use CEHRT remains.

b. Examples of Enforcement:

   i. CareCloud Health, Inc.: In April 2021, CareCloud agreed to pay $3.8 million to settle allegations related to its "Champion Program", through which it allegedly offered clients cash equivalent credits, cash bonuses, and percentage success payments to recommend CareCloud products and required clients not to provide negative information about the products.

   ii. Athenahealth Inc.: In January 2021, EHR developer athenahealth, Inc. agreed to pay $18.25 million to resolve allegations that it violated the FCA by paying illegal kickbacks to generate sales of its EHR product by inviting prospects and customers to all-expenses-paid sporting, entertainment, and recreational events, paying illegal fees to its customers through its "Lead Generation" program designed to identify new prospective customers, and entering into deals with competing companies that had decided to discontinue their health IT products under which the competing companies agreed to refer their clients to Athena in exchange for payments based on the value and volume of practices that were successfully converted into Athena customers.

   iii. Practice Fusion Inc.: In January 2020, Practice Fusion Inc. agreed to pay $145.0 million to resolve allegations that it accepted kickbacks from an opioid manufacturer and other pharmaceutical companies in exchange for implementing clinical decision support alerts in its EHR software, which were designed to increase prescriptions for the drug companies' products, and caused its users to submit false claims for federal incentive payments by misrepresenting the capabilities of its EHR software.

   iv. Greenway Health, LLC: Greenway Health entered into a FCA settlement agreement wherein it agreed to pay $57.25 million for falsely representing in the ONC certification process that its EHR product complied with all applicable requirements under the ONC Health IT Certification Program,

despite knowing that its product, Prime Suite, would not satisfy all such requirements. As a result, Greenway Health caused its customers to falsely attest to compliance with CMS requirements necessary to receive incentive payments for the use of CEHRT. In addition, Greenway Health allegedly knowingly caused users to report inaccurate information regarding Meaningful Use objectives and measures in attestations to CMS and state Medicaid agencies for purposes of obtaining incentive payments and provided improper remuneration to healthcare providers to continue using their EHR product and to recommend it to other users.

v. eClinicalWorks: eClinicalWorks and three of its senior executives agreed to pay $155 million to settle allegations related to causing health care providers to submit false claims to the Medicare and Medicaid EHR Incentive Programs by concealing from its customers that its software did not comply with CEHRT requirements. The company's alleged failure to comply with requirements to use standardized drug codes, to accurately record user actions in an audit log, and to always accurately record diagnostic imaging orders or perform drug interaction checks could also have posed potential risks to patient safety.

c. Advisory Opinions:

i. OIG Advisory Opinion No. 14-03: In April 2014, OIG issued an advisory opinion that rescinded Advisory Opinion 11-18 related to EHR interfaces that allow clinicians to refer patients. In this advisory opinion, a laboratory inquired about an arrangement with an EHR vendor under which the laboratory would pay a per-order fee for each test order the vendor transmits to the laboratory. OIG responded that this arrangement could result in prohibited remuneration under the Anti-Kickback Statute and could result in administrative sanctions because, under the arrangement, referring physicians would not incur transmission fees when they use the EHR to refer to "in-network" providers, practitioners, or suppliers. OIG noted that this feature of the arrangement could have the effect of influencing referral decisions in a material way and that there appeared to be no other reason for the per-order fees other than to secure referrals.

Recommendations and Compliance Strategies

A. Structuring Deals and Relationships

a. Assess Potential Kickbacks for Referrals: Generally speaking, any arrangements with physicians, health systems, or others that may receive reimbursement from the Federal health care programs - or sell items or services that may directly or indirectly reimbursed by the Federal health care programs - should be reviewed to assess whether there is payment or another kind of remuneration in exchange for referring, purchasing, leasing, recommending, or arranging for the referral,

purchase, lease, or recommendation of any item or service that may ultimately be payable by the Federal health care programs. Risk may be highest when arrangements relate to items and services directly billed to the Federal health care programs, but even for items and services that are not billed directly, fraud and abuse laws may be triggered by potential cost allocation and accounting by physicians and health systems. It is also important to review arrangements for compliance with state anti-kickback and fee-splitting laws, some of which may have a broader scope than the AKS. With respect to arrangements related to clinical laboratories or substance abuse recovery facilities, also consider the impact of the Eliminating Kickbacks in Recovery Act ("EKRA"). In short, if a purpose or effect of an arrangement is to increase the volume ordered or sold of health care items or services or health care related business - or to direct that business toward a particular entity or entities over others - the arrangement should be carefully scrutinized for regulatory risk and structured with an eye toward compliance with applicable safe harbors and exceptions.

b. Ask Operative Questions: In gathering information for any potential deal or other arrangement where fraud and abuse laws may be implicated, consider asking the following questions:

Assessing applicability of fraud and abuse laws:

i. Are any items or services related to the arrangement reimbursable, directly or indirectly, under a Federal health care program?

ii. As part of a provider's cost accounting, could any funds from a Federal health care program be applied to items or services that are a part of the arrangement?

iii. Do the items or services related to the arrangement trigger the application of state law or EKRA?

iv. What other types of arrangements exist between the parties?

v. Are any individuals or individual relationships compensated (e.g. compensation to a physician)?

Structuring arrangements with potential fraud and abuse implications:

i. Will there be a written, signed agreement?

ii. Does the agreement cover all services that are a part of the arrangement?

iii. How is compensation structured under the arrangement? Who is getting paid what, and how are fees determined?

iv. Are all associated fees based on fair market value and reflected in the agreement?

v. Will there be any free or discounted items or services as part of the arrangement? Why are these being offered?

vi. Is the compensation methodology structured such that a party or parties make more money when more business is generated under the arrangement?

vii. What are the parties' goals and purposes in structuring the arrangement? Are these permissible? Are any revisions to the structure required to clearly and accurately reflect permissible purposes?

viii. What safeguards can and should the parties adopt to minimize risk of violating applicable laws? Carve-outs (but see OIG commentary)? Limitations on referrals? Oversight/metrics? Others?

c. Special Considerations for Joint Arrangements Involving Multiple Parties: Arrangements involving multiple parties may require a more complex analysis, including obtaining clarity on which parties may be paying for the arrangement, providing technology or related technical services, or receiving the benefits from the arrangement.

i. Advisory Opinion No. 17-07: OIG opined that a pharmaceutical manufacturer, industry association, and a technology vendor collaborating with hospital system and a Medicare Advantage plan ("MA Plan") as part of a pilot program to fund, implement, and evaluate technology used for real-time electronic access to patient discharge information of MA Plan beneficiaries by MA Plan pharmacists although could generate potentially prohibited remuneration, would not cause the OIG to impose sanctions. In this arrangement, the pharmaceutical manufacturer would be contributing the funds, the industry association would be providing project management services, while the technology vendor would be providing the technology and related technical services. OIG based its decision on the following factors: (1) the proposed arrangement included numerous safeguards, including that the pharmaceutical manufacturer certified that agreements and operative documents would make clear that collaboration under this pilot would have no direct or indirect bearing on formulary recommendations or referrals of business; its involvement would be limited to funding and performing certain legal and compliance services; and it would have no involvement in selecting data points to be used, have no access to the technology or underlying data, and leave all pilot materials and technology unbranded, (2) the arrangement would be unlikely to lead to increased costs or overutilization of federally reimbursable services because the MA Plan has a strong incentive for its

members to receive the most appropriate and cost-effective treatment, (3) there would be little interference with clinical decision-making as pharmacists will not recommend one product over another, (4) there is unlikely to be a negative impact on care as the purpose of the pilot program is to improve the quality of care, and (5) the proposed arrangement is limited in number of patients and monetary investment.

B. Marketing

a. Marketing of federally reimbursable items or services, and in some cases other health care items and services, may pose risk for both the seller and the marketer. Risk may be elevated where marketing is performed by physicians or other health care providers who are in a position of patient trust. As such, consider training on how appropriate interactions should look. Carefully consider how marketer compensation is structured for compliance with applicable laws. Consider whether any commission-based marketer payments can be appropriate in view of at least the following considerations: (1) the types of items and services marketed, (2) whether the marketer is an employee or independent contractor, (3) whether the marketer is a clinician, and (4) the level of interaction between the marketer and patients.

b. Additionally, technology can be leveraged for marketing purposes, but organizations should be mindful to avoid any undue influence in recommending products or services using the technology, including in the design of any underlying algorithms. Moreover, any marketing should not target only federal health care program beneficiaries, but the broader population. OIG issued an advisory opinion in 2019 with additional guidance:

i. OIG Advisory Opinion No. 19-04: A technology company's proposal to make visible to Federal health care program beneficiaries: (i) its online healthcare directory for searching and booking medical appointments, where healthcare professionals would pay per-click or per-booking fees to be listed in the directory; and (ii) sponsored advertisements on its online healthcare directory and third-party websites, where healthcare professionals would pay per-impression or per-click fees for such sponsored advertisements would not implicate the civil monetary provisions related to beneficiary inducements (Beneficiary Inducement CMP) and while the arrangement implicated the Anti-Kickback Statute (AKS), it posed a low risk of fraud and abuse under the AKS. OIG based it conclusion on the fact that: (1) fee amounts would be established in advance, the aggregate fees would not exceed fair market value and would not take into account the volume or value of any business actually generated, and while more clicks or new-patient bookings would result in higher total fees for providers, fees would not be adjusted based on whether patients actually arrived for appointments or on the volume of

services patients used and the payment of higher fees due to more clicks would not result in more frequent appearances of a provider's name and information; (2) the technology company is not a provider or supplier, so there would not be any undue influence on patients when recommending items or services; (3) any display of sponsored results and general advertisements would not target federal health care program beneficiaries; (4) the marketing activity would not relate to any specific items or services users may obtain from providers as a result of appointments booked through the directory; (5) the potential user base is the general public regardless of insurance status; and (6) the technology company would not provide anything of value to Federal health care program beneficiaries other than inherent functionality and convenience.

c. Where PHI is involved, also consider limitations under HIPAA's Marketing Rule, which requires an individual's written authorization before a use or disclosure of his or her protected health information can be made for marketing with limited exceptions. *See* 45 C.F.R. 164.501 and 164.508(a)(3).

d. Industry organizations, such as Advanced Medical Technology Manufacturers Association (AdvaMed) and PhRMA have published codes for interacting with health care professionals for companies that develop, manufacture, and market medical products and technologies, including guidance on reviewing and structuring arrangements or relationships with health care professionals. *See* PhRMA Code on Interactions with Healthcare Professionals and the AdvaMed Code of Ethics.

C. Internal Controls

a. Some organizations in the health care industry may be required to have or may benefit from the adoption of an effective compliance program. For instance, the OIG has issued model compliance guidance documents for several types of organizations, including hospitals, durable medical equipment companies, individual and small group practices, and pharmaceutical manufacturers. Moreover, the Federal Sentencing Guidelines encourage the adoption of a compliance program by allowing for the reduction of any sanctions imposed.

b. Effective compliance programs, including within health care, contain the following seven pillars:

i. Compliance standards and procedures;

ii. High-level responsibility;

iii. Employee screening;

iv. Educational programs;

v. Monitoring and auditing;

vi. Discipline and enforcement; and

vii. Response and prevention.