AHLA

March 2019 Volume 23 Issue 3

connections

For the health and life sciences law community

Telehealth Growth = Expansion of Fraud & Abuse Enforcement–*page 10*

Tough Decisions Ahead: When Is Hospital Closure the Right Decision?–*page 18*

Compliance Corner–*page 29*

OFFICIAL MAGAZINE OF AMERICAN HEALTH LAWYERS ASSOCIATION

Increased use of telehealth technologies for the provision of health care services is due to a variety of reasons, including a growing aging population, a nationwide shortage of health care providers, as well as evolving and increasingly sophisticated health care technology. Telehealth services are considered a cost-effective way to provide needed health care services to patients, and many patients are attracted to its convenience.

As the number of telehealth services available to be provided, and reimbursed for, has increased, enforcement agencies have placed more scrutiny on the regulation and distribution of these services to ensure they are provided in compliance with applicable fraud and abuse laws and regulations. Government enforcement in the telehealth space is certain only to grow as utilization of these services increases. This article explores certain elements of the regulatory background for telehealth providers and common themes from administrative, civil, and criminal enforcement actions, in addition to presenting suggestions for avoiding problematic arrangements.

Telehealth: Regulatory Considerations[1]

Although telehealth technology is an increasingly popular option for providing health care services, practitioners must first address a number of potential regulatory issues and questions. Each state separately regulates the provision of telehealth services, necessitating a state-by-state regulatory review and analysis of various potential barriers to entry. Unsurprisingly, these regulatory considerations often are a starting point for potential enforcement inquiry and activity at the state and federal levels. The following are examples of some of the key regulatory issues that providers must contemplate:

Cross-State Practice. With greater use of telehealth technology, state professional boards have had to consider the provision of health care services by physicians who are not physically located in the state but who are providing services to patients located in the state. Generally, state professional licensing boards require that any practitioner providing telehealth services hold a valid and unrestricted license in the state where the patient is located, even if the practitioner is not physically located in that state.

Establishing Provider-Patient Relationships. Most states require that practitioners and patients have an established "relationship" as a precursor to practitioners providing treatment. Traditionally, this meant that a practitioner has had an in-person encounter with the patient, but in many states this requirement has evolved to focus on the existence, prior to provision of telehealth services, of certain key factors such as a patient's medical history and the practitioner's affirmative acts (i.e., whether a practitioner is examining, diagnosing, treating, or agreeing to treat a patient).

Remote Prescribing. State professional and pharmacy boards have incorporated various rules and requirements for the remote prescribing of drugs, often addressing prescribing of controlled and non-controlled substances separately. These laws continue to evolve and there is a high degree of variation among states in addressing the issue of remote prescribing. The most restrictive states require an in-person evaluation or physical examination occur *before* permitting remote prescribing of drugs. More permissive states now allow remote prescribing of drugs without requiring in-person contact, but nonetheless require interaction between the practitioner and the patient, often in the form of a "face-to-face" remote encounter. All states prohibit the remote prescribing of drugs based solely on a patient's completion and submission of an online questionnaire.

Coverage and Reimbursement. Coverage of telehealth services by federal, state, and even commercial payers has increased as telehealth has become more widely accepted. Medicare, Medicaid, and a wide variety of commercial payers have established unique coverage and reimbursement criteria for telehealth services. However, these criteria often are inconsistent and not necessarily comprehensive, further adding a layer of complexity for telehealth providers seeking payment.

An Introduction to Telehealth Fraud and Abuse/ Enforcement Considerations

Specific to the provision of telehealth services, certain arrangements to provide such services generate questions and sometimes concerns about whether fraud and abuse laws are triggered, including the costs of telehealth technology and infrastructure, the potential for free and/or discounted technology equipment offered to distant site providers, the potential for free and/or discounted telehealth services provided by health care practitioners, and collection and payment of fees to third parties such as technology vendors and/or management companies. While fact-specific, these types of factors may implicate the federal Anti-Kickback Statute,[2] federal Physician Self-Referral (Stark) Law,[3] the False Claims Act,[4] and state-specific equivalents, including state "all payer" laws.

As the number of telehealth services available to be provided, and reimbursed for, has increased, enforcement agencies have placed more scrutiny on the regulation and distribution of these services to ensure they are provided in compliance with applicable fraud and abuse laws and regulations.

With increased coverage of and reimbursement for telehealth services comes increased potential risk for fraud and abuse committed by individuals and entities delivering these services. The first False Claims Act action against a telehealth provider was brought in 2016[5] and signaled to telehealth practitioners nationwide that the Office of Inspector General (OIG) is aware of attempts to defraud federal and state programs through the provision of telehealth services and likely will begin to hold providers of these services more accountable for compliance with laws and regulations.

Who Are the Enforcers? A multitude of federal and state enforcement agencies regularly focus fraud, waste, and abuse prevention efforts on the health care industry because of the amount of money at stake. Agencies including the U.S. Department of Justice, the OIG, the Centers for Medicare & Medicaid Services (CMS), the Drug Enforcement Administration (DEA), the Federal Trade Commission, state Medicaid Fraud Control Units, state professional boards, and even individual private citizens (known as whistleblowers), all take part in pursuing, investigating, and resolving matters involving potential health care fraud, waste, and abuse.

OIG Advisory Guidance Regarding Telehealth. Since 1997, the OIG has issued numerous advisory opinions discussing the applicability of the federal fraud and abuse laws to various types of health care-focused arrangements. Common themes emerge in the five advisory opinions that discuss the provision of telehealth-focused arrangements. Per OIG:

- Free/discounted telehealth services/equipment are considered forms of remuneration.
- Increased utilization of telehealth can yield significant public benefits.
- Use of telehealth services is unlikely to increase costs to federal payers beyond what is paid for the same services when provided in-person.

Although the OIG has concluded in some of its advisory opinions that the federal Anti-Kickback Statute was implicated by the proposed arrangements, to date no sanctions have been imposed.

The OIG also has signaled its interest in reviewing claims for services rendered via telehealth by adding new telehealth-focused items to its annual Work Plan.[6] In November 2017, the OIG announced a project to review selected states' Medicaid payments for telehealth services to determine whether the payments were allowable under federal Medicaid requirements and were made in conformance with the particular state's laws.[7] In April 2018, the OIG published a report based on an October 2017 Work Plan project to review Medicare payments for telehealth services, with specific focus on claims paid for telehealth services at distant sites that did not have corresponding claims from originating sites.[8]

Enforcement Roles of Pharmacists and PBMs. While physicians are responsible for compliance with state telehealth laws, including those related to the proper prescribing of drugs, both federal and state laws have placed certain levels of responsibility on pharmacists to exercise professional judgment when making a determination concerning the legitimacy of a prescription.[9] DEA regulations state that pharmacists have a "corresponding responsibility" to ensure a prescription for a controlled substance is valid, and that pharmacists who knowingly fill prescriptions not issued "in the usual course of professional treatment or in legitimate and authorized research" are subject to penalties.[10] To satisfy the pharmacist's responsibility, the DEA expects pharmacists to identify and resolve certain "red flags" to determine whether a controlled substance prescription is legitimate.[11] State boards of pharmacy have adopted similar regulations applicable to *all* prescription drugs requiring pharmacists to make reasonable efforts to ensure that prescriptions were issued for a legitimate medical purpose.[12]

The responsibility of pharmacists under federal and state laws to identify red flags and implement safeguards to ensure the legitimacy of prescriptions has evolved to adapt to changing technologies, including the increased issuance of prescriptions generated from telehealth encounters. Although more clarity is needed in the current law, certain states have provided guidance that makes clear that pharmacists may not turn a "blind eye" to illegitimate or fraudulent telehealth prescriptions. For example, the North Carolina Board of Pharmacy has issued guidance on its website stating that a pharmacist may not dispense a prescription generated from a telehealth encounter if "in the exercise of professional judgment, there is or reasonably may be a question regarding the order's accuracy validity, authenticity, or safety for the patient."[13] In addition, the Texas Board of Pharmacy has issued telehealth guidance discussing what constitutes a "reasonable effort" to determine if a valid patient-practitioner relationship exists.[14]

As the stakeholder that administers government-sponsored and commercial pharmacy benefit plans, pharmacy benefit managers (PBMs) have a strong interest in identifying and preventing fraudulent prescriptions generated from telehealth encounters. Due to their access to prescription claims submitted by thousands of pharmacies, CMS relies on Part D sponsors and their PBMs to be the first line of defense against fraud, waste, and abuse.[15] The Medicare Part D program requires Part D sponsors to ensure their PBMs implement a robust compliance program that includes an effective system for routine auditing and monitoring of prescription drug claims to identify fraudulent activity.[16] PBMs are expected to

With increased coverage of and reimbursement for telehealth services comes increased potential risk for fraud and abuse committed by individuals and entities delivering these services.

conduct real-time audits to catch fraud prior to the dispensing and utilize new data analytics technology that targets potential fraud in areas prone to abuse. Effective April 1, 2019, Part D sponsors and their PBMs will be required to reject pharmacy claims for drugs prescribed by individuals on CMS' published preclusion list.[17]

An Overview of Recent Enforcement Involving Telehealth Schemes

Much of the current telehealth-focused enforcement activity—both civil and criminal—is related to the remote prescribing of compounded medications. The Fiscal Year 2017 OIG Work Plan noted that Medicare Part D spending for compounded topical drugs grew by more than 3,400% between 2006 and 2015, reaching $224 million. Similarly, in 2010, the TRICARE program paid $23 million for compounded drugs, but these costs skyrocketed to $1.7 billion in the first nine months of 2015 before new controls went into effect.[18] This growth in spending, combined with an increase in the number of investigative cases involving compounded drugs, suggests the emergence of a significant fraud risk.

Common Elements of Drug Compounding Schemes. Pharmacists create compounded medications through the combining, mixing, or altering of the ingredients of a single, or sometimes multiple, drug(s), to create a drug tailored to the needs of an individual patient. Compounded drugs tend to be more expensive than non-compounded drugs, making them an attractive target for those engaged in fraud and abuse.

Investigators have identified some common, telltale signs of fraud in drug compounding schemes, including:

- Use of preprinted forms that have incorrect office addresses (including states where a prescriber is not licensed);
- Prescribers writing prescriptions for individuals in numerous states (including states where a prescriber is not licensed);
- Multiple, identical prescriptions written by the same prescribing provider, despite patients' ages, conditions, diagnoses, allergies, etc.;
- Prescribers writing identical prescriptions for multiple family members;
- Prescribers writing prescriptions for "marketers";
- Prescribers writing prescriptions containing basic mistakes (e.g., incorrectly spelling their own name, failing to complete prescriptions); and
- Prescriptions filled by patients who may not want/need prescribed medications.

Below are examples of recent telehealth enforcement actions:

United States v. Roix. In October 2018, four individuals and seven companies were indicted on 32 counts for an alleged conspiracy to commit health care fraud, mail fraud, and introducing misbranded drugs into interstate commerce. Defendants include a telehealth company and its chief executive officer (CEO), and the alleged scheme involves improperly solicited prescriptions for pain creams that allegedly resulted in almost $1 billion in fraudulent claims. Allegedly, defendants fraudulently solicited insurance coverage information and prescriptions from consumers nationwide. Both the telehealth company and its CEO pleaded guilty.[19]

Much of the current telehealth-focused enforcement activity—both civil and criminal—is related to the remote prescribing of compounded medications.

United States v. Cesario. Twelve defendants were charged with conspiracy to commit health care fraud and wire fraud for allegedly paying kickbacks to prescribing physicians, telemarketers, and TRICARE beneficiaries. Under the scheme, beneficiaries were paid "grants" for participating in a "medical study" for which they obtained and filled compounded drug prescriptions through defendants' pharmacies. The scheme allegedly resulted in nearly $100 million in losses to the federal government over two years. In October 2017, one defendant pleaded guilty to conspiracy to commit health care fraud and admitted to conspiring with the scheme's masterminds to defraud the TRICARE program. The trial for the remaining defendants has not yet been scheduled.[20]

United States v. Grow. Grow involves a pharmacy telemarketing company that allegedly recruited TRICARE beneficiaries to order compounded prescription medications. The company operator was charged with conspiracy to commit health care fraud, payment and receipt of kickbacks, and money laundering. Grow, along with others, paid kickbacks to telehealth companies in exchange for recruiting and referring TRICARE beneficiaries without physical examinations or the establishment of legitimate physician-patient relationships. In less than one year, Grow and his co-defendants allegedly received over $20 million in kickbacks from a co-conspirator compounding pharmacy. Grow was convicted in February 2018, sentenced to 22 years in prison, and required to pay $18 million in restitution. By April 2018, eight of Grow's co-conspirators had pleaded guilty to federal criminal charges arising from Grow's fraudulent scheme.[21]

United States v. Powers. Defendant-physicians were charged for allegedly operating a scheme involving an online telehealth portal that promoted the sale of compounded medications. They allegedly recruited physicians to review patient files that defendants falsely claimed were prepared by other, qualified practitioners, and then used the reviewing physicians' identities and medical credentials to authorize the compounded medication prescriptions. Both defendants currently await trial.[22]

There have been other state and administrative enforcement efforts as well involving the provision of allegedly inappropriate prescriptions to patients, such as:

Hageseth v. Superior Court. In 2007, the California Court of Appeal heard a case involving a defendant physician who contracted with a web-based prescription services company to review patients' responses to online questionnaires and prescribe medications despite never interacting with the patients. The California Medical Board initiated an investigation into the physician's practice and referred the matter to the California Attorney General. The physician was charged with the felony of willfully and unlawfully practicing medicine without a license in California and sentenced to a nine-month prison term.[23]

Golob v. Arizona Medical Board. Arizona's state medical board sanctioned a physician for issuing prescriptions based almost exclusively on individuals' answers to online questionnaires. The physician issued more than 9,000 prescriptions in this manner between February and July of 2004. The Arizona Medical Board determined that the physician issued these prescriptions without establishing valid physician-patient relationships and issued sanctions that included a Decree of Censure. The physician challenged the board's determination in court, but the Arizona Court of Appeals ultimately affirmed the sanctions.[24]

Telehealth providers should be on high alert for partnerships with telehealth companies that would generate easy money for the practice.

Suggestions for Avoiding Fraudulent Telehealth Arrangements

The telehealth industry has solidified its role as an integral and progressive element of the U.S. health care system. Just as providers, telehealth companies, and even consumers must be mindful of the various regulatory barriers to telepractice, so too must stakeholders be careful of potential enforcement risks and continuously monitor regulatory developments at both the federal and state levels.

Telehealth providers should be on high alert for partnerships with telehealth companies that would generate easy money for the practice. Providers should ask basic questions when entering into such arrangements, including:

- Can you identify the address of where the telehealth company is located?
- Can you identify the first and last names of anyone who works at the telehealth company?
- Did you go through any hiring process other than submitting basic Human Resources paperwork?
- What training/oversight did you receive from the telehealth company?
- What is the extent of your compliance, Health Insurance Portability and Accountability Act, and fraud/waste/abuse training?
- Do you know the people you are working with, i.e., have you met them in-person?
- Are you required to speak with patients and conduct sufficient medical evaluations?
- What are the sources of your payments (i.e., insurance)?

Physicians will not be shielded from enforcement actions because of willful blindness or conscious avoidance. Physicians must actively monitor arrangement operations with an eye for signs of fraud or abuse as telehealth arrangements continue to grow. C

Alan J. Arville is a Member of the Firm in the Health Care and Life Sciences practice, in the Washington, DC, office of Epstein Becker Green. Mr. Arville provides strategic, transactional, and regulatory guidance to the health care industry. Mr. Arville's legal practice primarily focuses on matters relating to the distribution, dispensing, and reimbursement of pharmaceuticals, including the Medicare Part D program, the Medicare Advantage program, the 340B Drug Discount Program, federal anti-kickback and anti-inducement laws, HIPAA privacy and security, health care licensing, drug purchase agreements, payer contracting, and affiliations and other collaborative arrangements. He can be reached at ajarville@ebglaw.com.

Melissa L. Jampol is a Member of the Firm in the Health Care and Life Sciences and Litigation practices, in the New York and Newark offices of Epstein Becker Green. A former federal and state prosecutor, Ms. Jampol represents health care organizations—including health care systems, physician group practices, pharmacies, clinical laboratories, and other health care providers—and their officers and directors, in a variety of enforcement matters at both the state and federal levels. She can be reached at mjampol@ebglaw.com.

Amy F. Lerman is a Member of the Firm in the Health Care and Life Sciences practice, in the Washington, DC, office of Epstein Becker Green. Ms. Lerman focuses her practice on a variety of regulatory and transactional health care matters, including telehealth and telemedicine, government investigations, corporate compliance, durable medical equipment, and Medicare program integrity auditing and monitoring. She represents a variety of health care

providers and organizations, as well as investors and other financial institutions that invest in or support the health care industry. She can be reached at alerman@ebglaw.com.

Audrey Davis is an Associate in the Health Care and Life Sciences practice, in the Washington, DC, office of Epstein Becker Green. She focuses her practice on food and drug law, fraud and abuse, health care compliance, and managed care issues. She can be reached at adavis@ebglaw.com.

Endnotes

1 Federal agencies, states, and commercial payers define the terms "telehealth" and "telemedicine" differently, sometimes utilizing one of these terms and in some cases utilizing both. Increasingly, the terms have become interchangeable vernacular and generally refer to two-way, real-time, interactive communications between an originating site (the patient's location) and a distant site (the practitioner's location) for the purpose of facilitating the delivery of health care services. In this article, we primarily refer to these services as "telehealth" and focus on regulatory issues as they relate to physicians.

2 42 U.S.C. § 1320a-7b(b).

3 42 U.S.C. § 1395nn.

4 31 U.S.C. §§ 3729–33.

5 U.S. Dep't of Justice, Press Release, *Danbury Physician and Mental Health Practice Pay $36,000 to Settle False Claims Act Allegations* (July 27, 2016), https://www.justice.gov/usao-ct/pr/danbury-physician-and-mental-health-practice-pay-36000-settle-false-claims-act.

6 Off. of Inspector Gen., U.S. Dep't of Health & Hum. Servs., *Active Work Plan Items*, https://oig.hhs.gov/reports-and-publications/workplan/active-item-table.asp (last accessed Nov. 27, 2018).

7 John Kaveney, et al., *Potential for Fraud and Abuse in the Administration of Telehealth Services*, A.B.A. (Sept. 27, 2018), https://www.americanbar.org/groups/health_law/publications/aba_health_esource/2017-2018/april2018/fraud/.

8 Office of Inspector Gen., U.S. Dep't of Health & Human Servs., Rep. A-05-16-00058, CMS Paid Practitioners for Telehealth Services That Did Not Meet Medicare Requirements (Apr. 2018).

9 21 C.F.R. § 1306.04. *See, e.g.*, Ind. Code § 856:2-6-2 (noting that it is the pharmacist's responsibility to be sure beyond a reasonable doubt that the practitioner issuing the prescription did so in good faith and has a valid DEA certificate of registration); Kan. Stat. Ann. § 65-1637 (describing pharmacists' responsibility to exercise professional judgment regarding validity and authenticity of any prescription order); Ga. Code Ann. § 480-27-.04 (directing pharmacists to exercise professional judgment regarding the accuracy and authenticity of prescription drug orders).

10 21 C.F.R. § 1306.04(a).

11 The DEA has discussed "red flags" in presentations, such as the March 2013 presentation titled *Combating Pharmaceutical Diversion* at the Pharmacy Diversion Awareness Conference, https://www.deadiversion.usdoj.gov/mtgs/pharm_awareness/conf_2013/march_2013/carter.pdf.

12 *E.g.*, 21 N.C. Admin. Code § 46.1801(b) (stating that pharmacists shall not fill a prescription order if, in the exercise of professional judgment, the validity of the order is questioned); Ohio Admin. Code § 4729-5-20 (describing the pharmacist's responsibility to determine the legitimacy of a prescription); Or. Admin. R. 855-019-0210 (requiring pharmacists to use professional judgment to determine the validity of prescriptions); 22 Tex. Admin. Code § 291.29(b) (requiring pharmacists to make every reasonable effort to determine prescription drug orders are issued for legitimate medical purposes).

13 N.C. Bd. of Pharmacy, *Frequently Asked Questions for Pharmacists on Prescriptions Generated By Telemedicine Encounters*, http://www.ncbop.org/faqs/Pharmacist/faq_PrescriptionsTelemedicine.htm (last accessed Dec. 3, 2018).

14 Texas St. Bd. of Pharmacy, *Telemedicine Frequently Asked Questions*, https://www.pharmacy.texas.gov/files_pdf/Telemedicine_FAQ.pdf (last accessed Dec. 3, 2018).

15 Office of Inspector Gen., U.S. Dep't of Health & Human Servs., Rep. OEI-02-16-00440, Questionable Billing for Compounded Topical Drugs in Medicare Part D (Aug. 2018).

16 Ctrs. for Medicare & Medicaid Servs., Prescription Drug Benefit Manual, Chapter 9, Compliance Program Guidelines (2013).

17 79 Fed. Reg. 29844 (2014); 80 Fed. Reg. 25958 (2015); 83 Fed. Reg. 16440 (2018). *See also* Ctrs. for Medicare & Medicaid Servs., *Preclusion List*, https://www.cms.gov/Medicare/Provider-Enrollment-and-Certification/MedicareProviderSupEnroll/PreclusionList.html (last accessed Feb. 6, 2019) (listing providers and prescribers precluded from receiving payment for Medicare Advantage items and services or Part D drugs).

18 U.S. Dep't of Health & Hum. Servs., Off. of Inspector Gen., OIG Work Plan 29 (2017), https://oig.hhs.gov/reports-and-publications/archives/workplan/2017/hhs%20oig%20work%20plan%202017.pdf.

19 No. 2:18-cr-00133 (E.D. Tenn. filed Sept. 14, 2018); U.S. Dep't of Justice, Press Release, *Four Men and Seven Companies Indicted for Billion-Dollar Telemedicine Fraud Conspiracy, Telemedicine Company and CEO Plead Guilty in Two Fraud Schemes* (Oct. 15, 2018), https://www.justice.gov/usao-edtn/pr/four-men-and-seven-companies-indicted-billion-dollar-telemedicine-fraud-conspiracy.

20 No. 3:16-cr-00060 (N.D. Tex. filed Feb. 23, 2016).

21 No. 1:16-cr-20893 (S.D. Fla. filed Jan. 26, 2016).

22 No. 8:17-cr-00077 (C.D. Cal. filed June 18, 2017).

23 59 Cal. Rptr. 3d 385 (Cal. Ct. App. 2007).

24 No. 1 CA-CV 07-0006 (Ariz. Ct. App. 2008).

Thanks go out to the leaders of the Fraud and Abuse Practice Group for contributing this feature article: **Gary W. Herschman**, Epstein Becker & Green PC, Newark, NJ (Chair); **Jacqueline C. Baratian**, Alston & Bird LLP, Washington, DC (Vice Chair—Research & Website); **Joseph M. Kahn**, Hall Render Killian Heath & Lyman PC, Morrisville, NC (Vice Chair—Publications); **Tony R. Maida**, McDermott Will & Emery LLP, New York, NY (Vice Chair—Membership); **Caitlin Suzanne McCormick-Brault**, Columbia, MD (Vice Chair—Educational Programs); **Kevin E. Raphael**, Pietragallo Gordon Alfano Bosick & Raspanti LLP, Philadelphia, PA (Vice Chair—Strategic Planning and Special Projects); and **Jacob Harper**, Morgan Lewis & Bockius LLP, Washington, DC (Social Media Coordinator).