manatt

SEPTEMBER 2021

Telehealth: Regulation, Compliance, Audit and Investigation

John Libby, Partner
Manatt, Phelps & Phillips, LLP
Frank LaPallo, Partner
Manatt, Phelps & Phillips, LLP

About the Authors

John Libby, partner at Manatt, Phelps & Phillips, LLP, a former Assistant U.S. Attorney, leads Manatt's investigations and white collar defense practice. He represents businesses, as well as their officers and directors, during criminal investigations and prosecutions, as well as complex civil litigation.

Frank LaPallo, partner at Manatt, Phelps & Phillips, LLP, focuses his practice on the representation of health care enterprises, including with regard to transactions, fraud and abuse, licensing and certification, and operational, regulatory and litigation matters, including with respect to enterprises engaged in telehealth.

About Manatt Health

Manatt Health integrates legal and consulting services to better meet the complex needs of clients across the health care system.

Combining legal excellence, firsthand experience in shaping public policy, sophisticated strategy insight and deep analytic capabilities, we provide uniquely valuable professional services to the full range of health industry players.

Our diverse team of more than 160 attorneys and consultants from Manatt, Phelps & Phillips, LLP, and its consulting subsidiary, Manatt Health Strategies, LLC, is passionate about helping our clients advance their business interests, fulfill their missions and lead health care into the future. For more information, visit https://www.manatt.com/Health or contact:

John Libby
Partner
Manatt, Phelps & Phillips, LLP
310.312.4342
jlibby@manatt.com

Frank LaPallo
Partner
Manatt, Phelps & Phillips, LLP
310.312.4391
flapallo@manatt.com

Telehealth: Regulation, Compliance, Audit and Investigation

Table of Contents

Telehealth: Regulation, Compliance, Audit and Investigation

I. Introduction

Use and acceptance of telehealth technologies have grown very substantially since the start of the COVID-19 pandemic.[1] This growth has been substantially facilitated by waivers and relaxations of existing rules that otherwise restrict both settings and arrangements in which telehealth is permitted and reimbursement for such care.[2] These developments amplified a prior trend toward increasing utilization of telehealth technologies across multiple settings.[3]

In health care, increased utilization of, and increased scope of reimbursement for, particular categories of caregiving are often followed by increased incidence of noncompliance and fraud. These developments result in increased attention from government enforcers and private whistleblowers. As well, the "tech" element of telehealth has drawn into the field entrepreneurs who often have less familiarity with the broad and deep regulatory schemes of the American health care system than more experienced industry participants. Inevitably, where large amounts of money are available, true scamsters (as distinguished from those who, acting in good faith, simply err) are drawn in; and their actions influence the regulatory scrutiny that those operating in good faith must endure. In addition, private equity seems to be drawn to funding both startups and established companies in the telehealth area, new ventures which will need to focus on the significant and evolving compliance requirements in this area.

In light of these developments, it is important for those operating in the telehealth space to be aware of the regulatory requirements and hurdles they face, develop robust compliance programs, and be prepared to investigate their own operations and employees when potential violations are discovered.

A. Defining Telehealth

Telehealth technologies help to facilitate care delivery in multiple settings. The table below identifies several of the most frequently used. The regulatory and compliance issues addressed below are, to varying degrees, implicated in all of them.

Provider-to-Provider Platforms				
Use Case	**Description**	**Timing**	**Video**	**Information Transferred**
1 eConsult	Templated communications, where primary care provider eConsults with specialist to share information and discuss patient care.	Asynchronous	No	Medical records and images
2 Virtual video consult	Distant specialist connects in real time to a provider/clinical setting to deliver a clinical service directly supporting the care of a patient (e.g., telestroke).	Synchronous	Yes	Medical records and images
3 eICU/TeleAcute	Remote covering clinicians use multiple modalities (video, monitor data) to follow a defined set of seriously ill patients.	Synchronous	Yes	Medical records, images and monitoring data
Direct-to-Consumer Platforms				
4 Second opinion	Patient-initiated electronic request for provider to give an opinion on a clinical case.	Asynchronous	No	Medical records and images
5 Remote-patient monitoring	Providers remotely monitor patients via connected/mHealth devices or PROs.	Synchronous	No	Monitoring data and patient-reported data
6 Video visit	Provider connects directly with patient via video to conduct equivalent of a visit.	Synchronous	Yes	None
7 eVisit	Provider connects with patient via email or secure messaging to provide clinical advice or support.	Asynchronous	No	Patient-reported data and images

Source: American Hospital Association, *Telehealth, A Path to Virtual Integrated Care*.

This chart alone indicates the various possible compliance issues that can arise in the telehealth setting. Is the transmission of patient health information (PHI) secure? Is a telehealth consult clinically appropriate? How are reimbursement rules requiring face-to-face interaction implicated, and which ones have been relaxed during the public health emergency (PHE)[4] declared during the pandemic? These and other issues will be addressed in the balance of this article.

B. Federal Enforcement Initiatives and Audit Activities

Enforcement attention on telehealth has been vigorous. Thus telehealth providers are well-advised to focus on compliance with regulatory requirements and risk assessment. Recent Office of Inspector General (OIG) of the Department of Health and Human Services (HHS) reports, enforcement actions and statements illustrate these points.

In 2018, the OIG reported on an audit of telehealth payments made by CMS based on a stratified random sample of 100 claims out of 191,118 Medicare-paid distant-site telehealth claims.[5] In the relevant period (2014–2015), 31 claims in the sample did not meet Medicare requirements for payment, including 24 claims where the originating sites were nonrural (and thus did not qualify for Medicare reimbursement as telehealth), and seven claims were billed by institutional providers that were not eligible to provide telehealth services.

In 2019 the OIG and the U.S. Department of Justice announced a major national takedown against telefraud, charging 24 defendants in 17 judicial districts with $1.7 billion in fraudulent Medicare claims, of which $900 million were paid. The alleged scheme involved 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 medically unnecessary back, shoulder, wrist and knee braces. Some of the defendants allegedly controlled an international telemarketing network that lured hundreds of thousands of elderly and/or disabled patients into a criminal scheme that crossed borders, involving call centers in the Philippines and throughout Latin America. The defendants allegedly paid doctors to prescribe DME either with no patient interaction or with only a brief telephonic conversation with patients they had never met or seen.[6]

In September 2020, the OIG announced the "2020 National Health Care Fraud Takedown,"[7] alleging a "marketing network that lured hundreds of thousands of unsuspecting individuals into a criminal scheme through telemarketing calls, direct mail, television advertisements, and internet pop-up advertisements." "Defendant telemedicine executives allegedly paid medical practitioners to order unnecessary durable medical equipment, genetic and other diagnostic testing, and medications, either without any patient interaction or with only a brief telephonic conversation with patients they had never met or seen." Often, the durable medical equipment, test results or medications "were not provided to the beneficiaries or were worthless to the patients and their actual primary care doctors, and the misdirection, fake diagnoses, and unneeded tests misled patients and delayed their chance to seek appropriate treatment for medical complaints." The largest amount of alleged fraud loss charged in connection with the cases announced—$4.5 billion in allegedly false and fraudulent claims submitted by more than 86 criminal defendants in 19 judicial districts—related to schemes involving telemedicine.

The OIG's current work plan includes numerous items addressed to telehealth: Medicaid—Telehealth Expansion During COVID-19 Emergency,[8] Use of Medicare Telehealth Services During the COVID-19 Pandemic,[9] Medicare Telehealth Services During the COVID-19 Pandemic: Program Integrity Risks,[10] Home Health Agencies' Challenges and Strategies in Responding to the COVID-19 Pandemic,[11] Audits of Medicare Part B Telehealth Services During the COVID-19 Public Health Emergency,[12] and Use of Telehealth to Provide

Behavioral Health Services in Medicaid Managed Care.[13] And in prepared remarks for the April 2021 HCCA Compliance Institute, OIG Principal Deputy Inspector General Grimm included "Realizing the Potential of Telehealth" as one of the OIG's ten key compliance priorities.[14]

Finally, lest legitimate providers infer that they are in the crosshairs, there is an indication that the OIG is able to distinguish blatant fraud schemes from the more typical errors that providers have made since the government became such a large payer of health care costs. Thus in February 2021, Principal Deputy Inspector General Grimm released a statement distinguishing between "telefraud" and "telehealth fraud":

"We are aware of concerns raised regarding enforcement actions related to 'telefraud' schemes, and it is important to distinguish those schemes from telehealth fraud. In the last few years, the OIG has conducted several large investigations of fraud schemes that inappropriately leveraged the reach of telemarketing schemes in combination with unscrupulous doctors conducting sham remote visits to increase the size and scale of the perpetrator's criminal operations. In many cases, the criminals did not bill for the sham telehealth visit. Instead, the perpetrators billed fraudulently for other items or services, like durable medical equipment or genetic tests. We will continue to vigilantly pursue these 'telefraud' schemes and monitor the evolution of scams that may relate to telehealth."[15]

II. Regulation of Telehealth

During the COVID-19 pandemic, both the federal and state governments implemented temporary waivers of many regulatory requirements relevant to telehealth. Except as otherwise noted, this article addresses regulatory provisions in effect before these waivers; i.e., the permanent rules. There has been considerable discussion of making some of the waivers permanent in the post-pandemic period.[16] Whether or not some or all of these waivers are made permanent—and that is by no means certain[17]—the regulatory issues discussed below will, to some degree, remain, and operators in the telehealth space will have to be aware of and address them. Finally, regulation of telehealth is changing at a rapid pace. Readers are well-advised to avail themselves of resources that monitor and report on such change.[18]

A. Professional Licensure

Persons engaged in the delivery of health care services are generally subject to state licensure laws. In the context of telehealth, the relevant inquiry is where is the patient located. Professional licensing laws are "consumer protection" laws intended to protect residents of a given state. Thus, in general, the provision of licensed professional services to a state's residents via telehealth requires a professional license issued by that state.[19] There are some exceptions for peer-to-peer consulting[20] and for limited interactions with a state's residents by a physician licensed in another state, including treatment by physicians licensed in a neighboring state who provide services to residents of the nearby state.[21] Finally, a few states issue special telehealth licenses or permit registrations that allow out-of-state providers to provide telehealth services to patients in state.[22]

Some states have statutes/rules applicable to telehealth that apply to professionals in multiple license categories.[23] Other states have telehealth rules/statutes that apply specifically to medicine.[24]

Various interstate compacts may facilitate the provision of telehealth services. These compacts are agreements among participating states to work together to streamline the licensing process for clinicians who want to practice in multiple states. There are compacts for medicine,[25] nursing,[26] physical therapy,[27] EMS personnel,[28] audiology and speech therapy[29] and psychology.[30] Except for the psychology pact, which is intended to allow licensed psychologists to practice telepsychology and conduct temporary in-person face-to-face practice of psychology across state boundaries without necessitating that an individual become licensed in every state to practice, the compacts do not in themselves allow a professional who is licensed in one participating state to practice in another state. Rather, they streamline the licensing process by which a professional licensed in a participating state can obtain a license from another participating state.[31]

B. Standard of Care/Patient Consent

The standard of care for health care services delivered via telehealth technologies is generally the same as for care delivered in person.[32] Similarly, patient consent is required to provide treatment. However, most states require some form of explicit patient consent to treatment via telehealth, either verbal or written,[33] and that consent should be documented in the encounter record. As with other telehealth regulatory considerations, the law/rules of the state of the patient's residence will apply. The key here is establishing the provider-patient relationship in compliance with state law.

C. Prescribing Drugs

Prescribing medication for patients is one of the most common acts of medical practice. Prescribing, dispensing or furnishing drugs is subject to varying requirements from state to state. Under California law, for example, it is unprofessional conduct for a physician to prescribe, dispense or furnish "dangerous" drugs (i.e., drugs bearing the legend that federal law prohibits dispensing without prescription without an appropriate prior examination and a medical indication).[34] In California, an appropriate prior examination does not require an in-person interaction between the patient and the licensee and can be achieved through the use of telehealth, including, but not limited to, a self-screening tool or a questionnaire, provided that the licensee complies with the appropriate standard of care. In Florida, a telehealth provider may use telehealth to perform a patient evaluation, but may not use telehealth to prescribe a controlled substance unless the controlled substance is prescribed for a psychiatric disorder, for inpatient treatment at a hospital, for a patient receiving hospice services or for the resident of a nursing home facility.[35] In most states an Internet/online questionnaire alone is inadequate to establish a patient-provider relationship for prescribing purposes.[36]

1. Controlled Substances

Under federal law, prescribers must be registered with the Drug Enforcement Administration to prescribe controlled substances.[37] As well, state laws impose requirements with respect to "secure prescription" forms[38] or official prescription forms[39] and obligations to check a controlled substance database before prescribing.[40]

2. Ryan Haight Online Pharmacy Consumer Protection Act of 2008

The Ryan Haight Online Pharmacy Consumer Protection Act of 2008 (Pub. L. 110-425) ("Ryan Haight Act" or "act"), enacted in 2008, amended the Controlled Substances Act by adding various provisions to prevent the illegal distribution and dispensing of controlled substances by means of the Internet. The act makes it illegal under federal law to "deliver, distribute, or dispense a controlled substance by means of the Internet, except as authorized by [the Controlled Substances Act]." The Ryan Haight Act was enacted to prevent "rogue websites" fueling the abuse of prescription controlled substances, setting out numerous regulatory requirements and other substantive provisions. The act mandates, with limited exceptions,[41] that the dispensing of controlled substances by means of the Internet be predicated on a valid prescription issued by a practitioner who has conducted at least one in-person medical evaluation of the patient. The act also added two new criminal offenses to the Controlled Substances Act: making it explicitly unlawful for any person to knowingly or intentionally dispense, distribute or deliver a controlled substance by means of the Internet or to aid and abet such actions; and prohibiting using the Internet to knowingly or intentionally advertise illegal transactions of controlled substances that are not authorized by the Controlled Substances Act.

Significantly, the act also provided a definition of the "practice of telemedicine"—practice "conducted by a practitioner who has obtained from the [DEA] Administrator a special registration under [21 U.S.C. 831(h)]." The act, as amended, contemplates that the DEA will issue regulations effectuating this telemedicine special registration provision by October 24, 2019. However, the DEA has not yet issued such regulations. Thus, but for the current exception applicable during the COVID public health emergency[42] (and the non-public health emergency exceptions referenced above and in the footnote), the prescribing practitioner must conduct at least one in-person medical evaluation of the patient before prescribing controlled substances.[43]

3. State Controlled Substance Regulations

States have enacted their own controlled substance regulations.[44] In some cases, state statutes or regulations restrict telehealth providers from prescribing controlled substances without an in-person visit.[45]

4. E-prescribing Requirements

Some states have enacted requirements that certain prescribers for controlled substances must conduct prescribing electronically (subject to specified exceptions).[46] Further, under Medicare Part D, prescribers must, except in circumstances in which the Secretary waives the requirement, conduct all prescribing for Schedule II, III, IV and V controlled substances electronically.[47]

5. Dispensing Drugs

Drug dispensing via mail or other shipment is part of the offerings of some direct-to-consumer telehealth providers. Dispensing of dangerous drugs generally requires a pharmacy license, although some states permit physicians to dispense drugs to their patients.[48] Some states have telepharmacy rules to allow remote site dispensing by an in-state pharmacy.[49] Out-of-state pharmacies typically must hold a license issued by the state in which the patient is located,[50] and some states require that the pharmacist-in-charge of such a pharmacy be licensed by the state in which the patient is located.[51]

D. Laboratory Regulation

Included in the business models of some telehealth providers are clinical laboratory services. These services may include tests to detect COVID-19 antibodies and other diagnostic testing. Clinical laboratories are regulated by CMS under the Clinical Laboratory Improvement Amendments of 1988[52] (CLIA), as well as by statutes and regulations in several states. If a state enacts clinical laboratory laws that provide for requirements equal to or more stringent than the requirements of CLIA, CMS may exempt clinical laboratories in that state from CLIA.[53] Two states, New York and Washington, are currently exempt.[54] Otherwise, CLIA certification is required for clinical laboratories offering laboratory testing to patients, and some nonexempt states also have laws and rules regulating clinical laboratories. CLIA certification is achieved through applications submitted to specified state agencies.[55] CLIA-certified clinical laboratories are subjected to extensive requirements in accordance with the complexity of tests performed (waived, moderate or high), including with respect to proficiency testing, specimen handling, personnel and quality controls.

An issue receiving increasing attention is "direct access testing" (DAT), in which a laboratory accepts a request to conduct a clinical laboratory test directly from a patient without a requirement for a physician order. Where DAT is permitted, it is commonly ordered by an individual without a prior consultation with a physician or a physician's request for testing. There is no restriction on DAT under CLIA.[56] States have varying approaches to DAT.[57]

E. Privacy and Security

1. Health Insurance Portability and Accountability Act (HIPAA)

If a telehealth provider is a HIPAA "covered entity" (i.e., an organization that furnishes, bills for or is paid for health care in the normal course of business and that transmits any health information in electronic form in connection with a HIPAA-covered transaction), HIPAA's privacy, security and breach notification rules apply.[58] With respect to telehealth technology platforms, it should be noted that there is no government certification of HIPAA compliance. Thus, telehealth providers must conduct their own HIPAA-required risk analysis,[59] and ensure that PHI is exchanged and maintained in a secure, compliant manner.

2. State Privacy Laws

Telehealth providers are also subject to state health care privacy laws. Health care privacy laws that are more stringent than HIPAA requirements are not preempted.[60] Thus, the prudent approach would be for the covered entity telehealth provider to employ whichever are the most stringent requirements applicable to its operations across its platform.

3. Foreign Privacy Laws

Laws of other countries can apply if the telehealth provider serves residents of those countries. For example the European Union General Data Protection Regulation[61] can apply if residents of the EU interact with a telehealth provider based in the United States.

F. ADA Compliance

The Americans with Disabilities Act (ADA)[62] requires accessibility for in-person health care.[63] Also, Section 1557 of the Affordable Care Act[64] and implementing regulations[65] provide that an individual shall not be excluded from participation in, be denied the benefits of or be subjected to discrimination on the grounds prohibited under, inter alia, the ADA. If the technology used by a telehealth provider does not make its services reasonably accessible to individuals with disabilities, liability under these statutes and regulations might result. In addition to enforcement by, among other agencies, the DHHS Office for Civil Rights, the Department of Justice and the Federal Communications Commission, private actions under the ADA are authorized.[66] In light of the foregoing, telehealth providers are well-advised to make reasonable efforts to make their services accessible to persons who are blind or have low vision, or are deaf or hard of hearing.

G. Practitioner Credentialing

As with any health care setting, operators of telehealth enterprises must assure that their providers have the licenses, competence and other qualifications to perform the services offered. Direct-to-consumer telehealth entities will credential their providers in a manner similar to the way in which comparable in-person operators credential their providers. Special credentialing issues arise where telemedicine services are provided to patients of one institution by physicians located at another institution. Both the Medicare conditions of participation for hospitals and the hospital accreditation standards of The Joint Commission (TJC) address this issue. Under Medicare hospital conditions of participation, a hospital ("originating site") receiving medical services from another hospital ("distant site") may rely on the credentialing performed by the distant site hospital if certain conditions are met.[67] A similar rule applies where the distant site is not a hospital.[68] The TJC medical staff accreditation standard allows a similar approach.[69]

H. Fraud and Abuse Laws

1. Anti-kickback Laws

The federal anti-kickback statute (AKS)[70] prohibits offering, paying, soliciting or receiving any remuneration for referrals of items or services for which payment may be made in whole or in part under a federal health care program. Violation of the AKS is a crime, and administrative penalties under the Civil Money Penalties Act, enforced by the OIG, are also authorized.[71] As well, states generally have anti-kickback statutes. In some cases these apply to all payers;[72] in other cases, they apply only to services covered by the state's Medicaid program.[73] Kickback exposure can arise in the context of telehealth, among other ways, where a telehealth enterprise offers filling of drug prescriptions or performing of clinical laboratory services by affiliated providers. Financial relationships between the ordering physician and the pharmacy or laboratory that fulfills these orders can implicate anti-kickback statutes. AKS exposure can also arise where remuneration is given to Medicare or Medicaid beneficiaries to induce them to utilize items or services covered by such programs.

2. Physician Self-Referral Laws

The federal Physician Self-Referral Law,[74] commonly referred to as the Stark Law, prohibits physicians from referring patients to receive "designated health services" payable by Medicare or Medicaid from entities with which the physician or an immediate family member has a financial relationship, unless an exception applies. Financial relationships include both ownership/investment interests and compensation arrangements. There are also state analogs to the Stark Law.[75] In the telehealth context, the Stark Law and state analog statutes could be implicated if a physician owner or employee of a telehealth business has a direct or indirect financial relationship with a laboratory or pharmacy and that physician orders laboratory services to be provided by the laboratory or drugs to be dispensed by the pharmacy.

3. Beneficiary Inducement Prohibition

The beneficiary inducement statute[76] prohibits offering or transferring any remuneration to a Medicare or Medicaid beneficiary if the remuneration is likely to influence the beneficiary's selection of a particular provider, practitioner or supplier of items or services paid for by Medicare or Medicaid. Violators may be liable for civil money penalties of up to $10,000 for each such item or service and up to three times the amount claimed for such item or service.[77] The statute is implicated in situations, among others, where a provider waives coinsurance or deductible amounts owed by a beneficiary. The regulations for this statute include several exceptions, most notably, waiver of coinsurance and deductible amounts by a person if the waiver is not offered as part of any advertisement or solicitation and the provider does not routinely waive coinsurance or deductible amounts; waiver of coinsurance and/or deductible amounts is made after the provider determines in good faith that the individual is in financial need; or a failure to collect coinsurance or deductible amounts after making reasonable collection efforts;[78] and provision of telehealth technologies by a provider of services, a physician or a renal dialysis facility to an individual with end-stage renal disease who is receiving home dialysis provided for the purpose of furnishing telehealth services related to the individual's end-stage renal disease, subject to certain conditions.[79]

4. False Claims Acts

The federal civil False Claims Act (FCA)[80] imposes civil and criminal liability on individuals or entities that knowingly submit false or fraudulent claims for payment to the government or knowingly make, or cause to be made, a false statement in order to have a false claim paid. Liability under the FCA can reach three times the amount of the loss to the relevant government program, including Medicare, Medicaid, Tricare and others, plus a civil penalty per claim filed, adjusted for inflation according to statute and regulation.[81] Under the civil FCA, each instance of an item or a service billed to Medicare or Medicaid counts as a claim, so monetary liability can quickly become quite substantial. Further, the fact that a claim results from an AKS violation or is made in violation of the Stark Law also may render it false or fraudulent, creating liability under the civil FCA (as well as under the AKS or Stark Law). The FCA provides for private actions on behalf of the government by whistleblowers (*qui tam* relators), who may share in recoveries. Thus, telehealth providers face potential exposure under the FCA for false billings to federal health care programs, as well as AKS or Stark Law violations; and the provision for actions by whistleblowers puts a premium on efforts to assure compliance.

Many states also have false claims statutes, including with provisions for actions brought by whistleblowers.[82]

5. Fee Splitting

Where a health care professional splits part of the professional fee earned from treating the referred patient with the source of the referral, the practice is often referred to as "fee splitting." About two-thirds of states have some form of fee-splitting prohibition. In some cases these appear to prohibit otherwise appropriate business relationships with entities that are not health care providers, such as billing agencies or management companies. Florida, New York, North Carolina and Tennessee have notably broad prohibitions against fee splitting. New York explicitly states that percentage-based agreements with billing companies are impermissible. Illinois law permits a percentage-based fee calculated on service fees billed. California permits such arrangements to be based on gross revenues.[83]

6. Coding and Billing

As with all health care endeavors, proper coding of services for which reimbursement is sought from third-party payers is crucial in telehealth. In addition to the usual issues of appropriate coding and billing for the acuity and complexity of the telehealth interaction, it is necessary to code properly for site of service, as well as to utilize relevant telehealth service coding modifiers. Different payers have different requirements for telehealth coding and following the applicable rules can be challenging. For example, in the absence of the PHE, Medicare limits coverage for telehealth services to certain types geographic areas where the patient is located ("originating site")[84] and certain types of settings.[85] On the other hand, for example, California's Medicaid program (Medi-Cal) does not limit the type of setting where services are provided for the patient or by the health care provider.[86] Similarly, Medicare limits the types of providers who can provide services via telehealth,[87] while Medi-Cal does not.[88] CMS publishes a list of CPT codes for approved Medicare fee-for-service payment for telehealth.[89] Finally, under Medicare there is a discrete set of technology-based services that are not deemed "telehealth" by CMS and not subject to the limitations that apply to telehealth services.[90]

7. Corporate Practice of Medicine

The corporate practice of medicine (CPOM) doctrine limits ownership and control of medical (and some other professional practices) to licensed professionals. To various degrees, the CPOM doctrine is in effect in approximately 30 states. Where a robust CPOM bar is in effect, as is the case in such states as California[91] and New York,[92] and where nonprofessional entities wish to participate in the relevant professional practice, a typical structure that is employed utilizes a management services organization with nonprofessional investors that contracts with a professional corporation or similar professional legal entity, typically owned by a "friendly" professional, to provide specifically identified services (which may include management, billing and other services, as well as personal property and real estate) for a fee. The arrangement may include some form of carefully articulated restriction on the ability of the friendly professional to dispose of the professional entity's equity ownership. Both the management fee and the ownership restriction arrangement must be carefully structured to avoid CPOM exposure. In certain states, decisions and activities such as scheduling, contracting, setting rates, and hiring and management of nonclinical personnel, as well as influence over clinical decisions, may implicate the restrictions on the corporate practice of medicine.[93]

8. Periodic Payment Models

Some direct-to-consumer telehealth businesses employ a "membership" model with reduced rates or access to certain specified services for a fixed periodic fee. This approach is somewhat analogous to "concierge" medicine. Where an entity agrees to provide or arrange for health care services in exchange for a fixed periodic payment, the question whether the arrangement constitutes "insurance" arises. In some states a periodic payment to arrange for or provide for health care subjects the entity to insurance regulation.[94] However, several states (e.g., Utah, Idaho, Montana, Oregon, Washington)[95] have enacted statutes providing that operation of "direct care" or "retainer" practices is not insurance. In these states, generally, provision of "primary care" for a periodic direct payment is deemed not to constitute "insurance." However, at least one state requires a retainer medical practice to be approved by the state.[96] In light of this, direct-to-consumer health care enterprises considering periodic or discount pricing models must consider these statutes in structuring their payment models.

III. Compliance and Investigations

Given the extensive and rapidly developing regulations concerning telehealth as well as its explosive growth since the COVID pandemic began in early 2020, it is important for telehealth providers to ensure that they have a robust compliance program in place that addresses these particular regulatory issues, as well as an understanding as to how to conduct independent and effective investigations should allegations of noncompliance, regulatory violations, or outright misconduct, fraud and abuse arise.

A. Elements of an Effective Compliance Program

The elements of an effective compliance program are well-known, and health care providers, whether an individual practitioner, large medical group or hospital, or telehealth startup or established company, will likely have at least implemented such a program. In order to have an effective compliance program, a telehealth provider must:

1. Establish standards and procedures to prevent and detect misconduct.
2. Ensure that its governing authority is knowledgeable about the content and operation of the compliance and ethics program and exercises reasonable oversight with respect to the implementation and effectiveness of the compliance and ethics program, including designating adequately resourced and independent personnel to carry out the compliance program.
3. Undertake reasonable efforts to exclude from high-level personnel any individual whom the organization knows, or should have known, through the exercise of due diligence, has engaged in illegal activities or other conduct inconsistent with an effective compliance and ethics program.
4. Undertake reasonable steps to communicate periodically and in a practical manner its standards and procedures and other aspects of the compliance and ethics program to employees and agents at all levels by conducting effective training programs and otherwise disseminating information appropriate to such individuals' respective roles and responsibilities.

5. Ensure the compliance program's effectiveness by monitoring and auditing to detect misconduct; periodically evaluate the program's effectiveness; and establish and publicize a hotline to allow for the anonymous reporting of actual or potential misconduct.
6. Promote and enforce the program consistently throughout the organization through (A) appropriate incentives to perform in accordance with the compliance and ethics program; and (B) appropriate disciplinary measures for engaging in misconduct and for failing to take reasonable steps to prevent or detect misconduct.
7. Ensure that once misconduct is detected, reasonable steps are taken to respond appropriately and to prevent further similar misconduct, including making any necessary modifications to the organization's compliance and ethics program.[97]

Especially for those providers which have transitioned to conducting more telehealth visits over the past two years, and intend to do so even after the pandemic is over, it is important to review any existing compliance plan to ensure that it takes into account these requirements, as well as to ensure its effective operation.

In the late 1990s and continuing into the 2000s, the OIG promulgated a series of compliance guidance documents for various sectors of the health care industry, including hospitals, nursing homes, pharma and physician practices.[98] While the government has not added any compliance guidance for many years, and has not done so for the telehealth sector, it is worth reviewing this guidance for those issues which the government does focus on in reviewing and evaluating compliance programs.

B. The Need for Prompt, Thorough and Independent Internal Investigations

Given the explosion of telehealth visits since the declaration of the pandemic in March 2020 as well as the rise in government funds to pay for these visits, it is likely that this new group of providers will come under increasing scrutiny by federal and state authorities. Allegations of fraud, misconduct, and violations of law and regulations can come from many sources: internal or hotline allegations, including by whistleblowers; media reports; civil litigation; regulatory examinations; or prosecutorial/law enforcement actions by federal, state or local prosecutors and regulators. Regulatory or law enforcement action can, in turn, take many forms, ranging from informal requests for documents and employee interviews, to subpoenas and civil investigative demands, to the execution of search warrants, to the filing of civil or criminal charges.

Each of these situations requires a certain level of investigation into the background facts, as the nature of the inquiry will likely vary depending on the source of the allegation. While internal, hotline and whistleblower complaints should all be taken seriously, the initial scope of the inquiry is likely to be relatively narrow, involving a defined scope of interviews and perhaps a limited review of documents. This scope will likely be expanded if the allegations appear to be substantiated. At the other end of the spectrum is formal action by the government, which will usually involve not only extensive investigation to identify, collect and produce responsive documents but also interviews with relevant employees with knowledge. The need to collect and review emails, either in response to a government document demand or for internal purposes, will further increase the scope (and expense) of any such investigation.

1. Government Policies Relating to Cooperation and Internal Investigations

There are several government policies and pronouncements which incentivize business organizations of all types and sizes to conduct thorough and independent investigations and to report the nonprivileged factual results to the government. At their heart, these policies and pronouncements stem from a fundamental quirk of U.S. law—the breadth of corporate criminal liability. In essence, a corporation, no matter how large, can be held criminally responsible for the conduct of even a low-level employee, if that employee was acting within the scope of their employment and with at least the partial intent to benefit the corporation.[99] Thus, regardless of the nature of the violation or the position of the employee within the organization, the company is at the mercy of the exercise of discretion by government prosecutors as to whether or not to charge the company, and what type of settlement to extract in view of the leverage the government enjoys.[100]

Government policies and pronouncements incentivizing companies to conduct internal investigations can all be traced back to the federal Organizational Sentencing Guidelines, initially promulgated in 1991, which provided for credit on federal criminal sentences for organizations that cooperate in government investigations, including promptly investigating and disclosing internal wrongdoing.[101] In several significant policy statements over the years since then, the U.S. Department of Justice has expanded these incentives to include cooperation credit for business organizations that are negotiating plea agreements, deferred prosecution agreements or nonprosecution agreements with the government. These policies are now embodied in the Federal Principles of Prosecution of Business Organizations section of Department of Justice's (DOJ) Justice Manual.[102] In addition, the DOJ's Criminal Division has promulgated related guidance, Evaluation of Corporate Compliance Programs.[103] For business organizations that have already entered into settlements with the government for prior wrongdoing, these settlements often include Corporate Integrity Agreements which impose further obligations on the organization to investigate and report allegations of wrongdoing. Cooperation in the form of the voluntary disclosure of facts concerning wrongdoing is a key factor in these policies, and of course such facts cannot be disclosed without a thorough and independent investigation to uncover them.

Another key element of cooperating with the government, as well as a prudential approach for business organizations to take, is to remediate or correct any issues noted during the course of the internal investigation.

While the government has often focused on corporate responsibility for violations of law and regulation, and insisted on the implementation of compliance programs, corporate integrity agreements and other ways to assure that such violations are prevented, detected, investigated, disclosed and corrected, it has also focused on individual responsibility for these violations, since corporations and other organizations can only act through individuals. This focus on individuals was formalized in September 2015 in a memo from then Deputy Attorney General Sally Yates titled "Individual Accountability for Corporate Wrongdoing," and clarified in 2018 by then Deputy Attorney General Rod Rosenstein. While for the most part the new policy conformed to prior practice in that, to qualify for cooperation credit, corporations must provide all relevant facts relating to individual misconduct, the original Yates memo also required all components of the DOJ, civil and criminal, to focus on individual misconduct and not solely corporate responsibility, and to coordinate such investigations.[104] The individual accountability policy also precluded the DOJ from releasing culpable individuals in a corporate resolution absent "extraordinary circumstances" and only then on the approval of

the relevant Assistant AG or U.S. Attorney. Deputy AG Rosenstein's 2018 pronouncement clarified that, while identification of culpable individuals was important, recovery of government funds and payments of fines were also important in corporate resolutions, and business organizations could continue to receive at least partial credit for providing facts relating to individual culpability even if the government disagreed with the nature and scope of such culpability and the number of individuals involved.

2. Client Imperatives in Conducting an Internal Investigation

Separate and apart from the incentives provided by various government regulations and policies as described above, clients often have strong incentives to conduct internal investigations. First, in the event of an exceptional event or allegation of corporate misconduct that is high-level or widespread, it is important for the board and senior management to have a clear view of the facts to inform further decision making. Second, outside actors—including regulators, auditors, activist shareholders and the media—will insist on accountability, which starts with understanding the facts in a clear and impartial way.[105] Third, a clear understanding of the facts will lead to "lessons learned" and remediation, including terminations of employees involved, civil litigation, voluntary disclosure to the government, and changed business processes, policies and procedures.

In short, conducting a thorough and independent internal investigation is simply part of good corporate governance. This holds true for telehealth providers, whether they are new startups or existing health systems seeing an expansion of this service.

C. Conducting the Investigation

1. Initial Steps: Defining the Scope, Establishing the Investigative Team, and Preserving and Collecting Documents

Once it is decided that an investigation is required, the key initial steps involve defining the scope of the investigation, establishing the team that will conduct the investigation, and ensuring the preservation and collection of key documents. This initial process will take place in conjunction with the independent individuals or body within the business organization that will oversee the investigation—this could be senior management, the board, or the Audit Committee or another board committee.

The scope of the investigation will largely be driven by the allegations that are being investigated and, as noted above, the source of those allegations. A key first step in the scoping process should thus include the preparation of a written, privileged document which should address the allegations along with the following issues:

a. Business lines or areas to be investigated
b. Legal framework
c. Questions to be answered
d. Categories of documents to be preserved, collected and reviewed
e. Individuals to be interviewed

f. Proposed timeline for completion

g. Form of final report

It should be understood, of course, that this scope document could change as the investigation proceeds—the scope could change, new key documents could be discovered, other witnesses could be identified for interview, new legal issues could emerge and timing could change. The scoping document, however, will provide guidance for the investigative team and the business organization's oversight body, and any changes will be carefully considered.

The next step is to define the investigative team. In most internal investigations the team should be led by counsel in order to retain privilege (unless and until there is a decision to waive privilege). In addition, most investigations of serious allegations, involving violations of law or regulations, should be done by reputable and experienced outside counsel in order to ensure that the investigation is done correctly, efficiently and ultimately to establish credibility with the government. In these circumstances in-house counsel will typically serve as outside counsel's liaison with the internal corporate body tasked with overseeing the investigation.

Depending on the nature and subject matter of the investigation, the team could also include private investigators; forensic accounting and data experts; experts in technology, including hardware or software; medical experts; or any other type of subject matter expert. Given the new and evolving nature of telehealth, there may be additional types of experts required.

These additional members of the investigative team will typically be retained by counsel and will be external to the business organization being investigated. However, where appropriate, independent subject matter experts within the organization and working at the clear direction of counsel can also be used.

The final critical initial step is ensuring that critical documents to be reviewed and used in witness interviews are preserved and collected. Again, the scoping process will be critical here in identifying which areas of the business, and therefore which custodians (and potential witnesses), should be the subject of a document hold. The scope of a document hold is likely to be broader than documents ultimately reviewed in connection with the investigation and/or produced to the government. The documents to be preserved will be driven by the nature of the investigation and the scope as defined by the investigative teams, and could include:

i. Governance documents

ii. Board books

iii. Policies and procedures

iv. Emails, texts, voicemails and other electronic documents

v. Medical records

vi. Billing records

vii. Recordings of telehealth visits, if any

The investigative team should retain an e-discovery vendor to assist in this process in order to understand the architecture of the organization's information technology infrastructure, the data and devices that need to be preserved and collected, and the scope of any document hold notice. For example, if all key documents and emails are preserved in the organization's servers and can be locked down and preserved without

additional actions by the individual custodians, then the scope of the notice can be limited. If, however, individual custodians have their own devices and the ability to save documents on those devices separate and apart from the organization's servers, then the scope should broaden to include those individuals. Finally, where specific individuals are identified as having been involved with the allegations of wrongdoing, their organization-issued devices should be seized, and any personal devices requested to be imaged, in order to preserve potentially critical evidence.

Failure to preserve documents can and will be considered by the government as a lack of cooperation and will likely adversely affect the organization's ability to resolve any government investigations favorably.[106] In extreme situations, failure to preserve documents that are ultimately destroyed could be prosecuted as obstruction of justice if done intentionally.[107]

2. Document Review

Once the documents are preserved and collected on a document review platform, the process of document review is ready to begin. There are likely to be many more documents preserved and collected than will ultimately be relevant to the investigation or responsive to government subpoenas or requests for information. Thus, a methodology for reducing the number of documents to be reviewed is necessary.

There are two generally accepted ways to do so—use of keyword searches, and machine learning or artificial intelligence. These approaches can be used independently or in combination to reduce the universe of documents that will be subject to human review. Especially in those cases where there is or will be a government investigation, it is important to carefully document the methodology used so that it can either be disclosed to or approved by the government in advance, or provided to the government after the fact.

Once the documents have been selected for human review, a protocol document should be prepared to train the reviewers and for their reference during their review. The protocol document will describe in general the nature of the investigation, the types of documents they will be reviewing, the issues to look for and when to tag documents for further review. The first-level set of reviewers are often entry-level attorneys or forensic professionals; their work will be subject to second-level review by more experienced professionals, including members of the investigative team. The reviewers will tag each document as either relevant or not relevant; will tag documents with issues as identified in the protocol document; and will identify key or "hot" documents based on the nature of the investigation and the issues involved.

3. Interviewing Witnesses

Once these initial steps are complete, and documents are collected and reviewed,[108] the next step is to interview the witnesses identified as part of the initial scoping process. If there are individual whistleblowers, they are likely to be interviewed first, sometimes even before the scoping process discussed above, and may end up being interviewed multiple times. On the other hand, any individuals who are the subjects of the investigation are likely to be interviewed last, once the investigation is nearly complete and they can be confronted with the results, if appropriate. Aside from these considerations, the witness order will be driven by numerous factors, including the scope, witnesses' schedules, and the need to learn key details from those lower down in the organizational hierarchy before interviewing those with more authority.

Interviews should be conducted with only a single witness at a time. At least two members of the investigative team should be present, including one of the lawyers and another person (lawyer, paralegal, investigator) to take notes and prepare a memorandum of the interview (MOI). Other members of the investigative team can be present as appropriate, especially if the subject matter of the interview will be technical and require the presence and expertise of one of the team's subject matter experts. However, it is important not to have too many people in the room so as not to overwhelm the witness and to create as informal and friendly an atmosphere as possible.

The lawyer leading the interview should begin by giving the witness the *Upjohn*[109] admonitions in order to set the ground rules for the interview and ensure that the witness understands those rules and how their statements could be used. The *Upjohn* admonitions consist of the following:[110]

- The lawyer's client is the witness's employer. The lawyer does not represent any individual employee of the employer, and specifically does not represent the witness.
- The interview is covered by the employer's attorney-client privilege with the lawyers since the witness is an employee of the employer and is being interviewed in that capacity. This means that the conversation is confidential. The witness should not disclose what is discussed with outside third parties in order to preserve the privilege and the integrity of the investigation.[111]
- The privilege belongs to the employer, which means only the employer can decide to disclose the discussion to a third party like the government or law enforcement.
- Notes are being taken and a memorandum of the interview is being prepared, and if the employer decides to waive the privilege either the memorandum or a summary could be disclosed.
- Does the employee have any questions or concerns?

After addressing any concerns the employee may have, the lawyer (and others present) will proceed with the interview. The note taker should note down just the facts relayed by the witness and not the question and answer format, including whether or not the witness knew a fact or not.

Once the interview is complete and the memorandum is prepared, members of the investigative team should review it for accuracy and completeness. The memo should not be shared with the witness, but if there is an area that requires clarification, the witness can be contacted and the clarification noted in a separate part of the same memo.

4. Liability Analysis

Once the investigation is complete, and likely before the results are reported to the client and the government, it would be appropriate to conduct a liability analysis to understand the extent to which the facts discovered constitute a violation of law and the extent to which the business organization and any individuals within the organization are responsible. The legal framework as set forth in the scoping document discussed above, as it may have evolved during the investigation, will inform the liability analysis and the ways in which the facts support or rebut a particular legal conclusion. The liability analysis should be objective as opposed to argumentative, and should set forth the risks to the organization and individuals based on the facts discovered during the investigation.

As discussed in the first part of this article, the legal landscape facing telehealth providers is complex and covers a wide variety of areas. Depending on the nature and scope of the allegations being investigated, the liability analysis will be correspondingly wide or narrow. In addition, as the law develops in this area, including settlements announced by the government, the liability analysis can be developed more robustly.

5. Report Results

Reporting the results of the internal investigation can take many forms. Typically, the audience for the reports will be the internal body of the business organization that commissioned and supervised the investigation to begin with. In addition, where the decision has been made to waive privilege as to the factual results of an investigation, the audience may include the government, and the disclosure of results may be a part of the business organization's effort to gain cooperation credit.

The form of the report will also vary, and will be dictated by the nature and scope of the investigation and the audience for the report. It could be verbal (based on the witness interviews and key documents gathered during the investigation), a PowerPoint or a full written narrative with attachments. The report could also be interim, based on the results of the investigation to date, or in a particular subject matter of the investigation.

Whatever form the report takes, it should address, at a minimum, the scope of the investigation and questions to be answered; documents preserved, collected and reviewed (including the methodology of the review); witnesses interviewed; and a factual narrative that answers the questions posed during the scoping process.

D. Responding to Government Investigations

The internal investigation process described above will typically run parallel to or precede a government investigation of the same or overlapping conduct. As noted above, the results of the internal investigation may be reported in some fashion to the government in an effort to gain cooperation credit and a more favorable resolution of any improper or illegal conduct.[112] Then the government also will seek to ensure that any policies, procedures, personnel or structural issues that led to the violation are corrected and reviewed on a periodic basis.[113]

A key aspect of responding to government investigations is managing the reactions and expectations of senior management and the board. Depending on the business organization and its leadership's level of sophistication in dealing with government investigations, the board and management may react with equanimity or panic. Counsel should of course do everything possible to move the needle back to the calm, businesslike side of the scale. Thus, individual members of the board and management should be told at the outset that counsel's client is the business organization, and not any individual, and that separate counsel will and should be retained for anyone who feels the need to have counsel in light of the nature and scope of the investigation (and, of course, such an individual cannot be part of the internal client team assisting outside counsel). Nonetheless, these individuals should also be told that all communications with counsel are confidential, and that the investigation should not be discussed outside the client team designated to manage the investigation. The board and management should also be told immediately that they should not delete or destroy any emails or other documents, nor should they trade the organization's securities as their actions may support an inference that the timing was based on knowledge of material inside information

concerning the investigation. There should also be no retaliation against any whistleblowers. Finally, the business organization should implement protocols to avoid conflicts of interest for legal, governance and operational aspects.

The presence of allegations of wrongdoing requiring an internal investigation, as well as a related government investigation, could create additional issues for the board and management, including the viability of continued operations in the area of the business affected by the investigation; balancing criminal and civil liability issues; ongoing remediation and risk management; and the costs of conducting an internal investigation, responding to the government and remediating violations.

Finally, it goes without saying that even if the government does not consider prompt and thorough compliance with subpoenas and other requests for information and documents to be cooperation, the business organization should strive to do so anyway. This does not mean the business organization should not push back on overly broad or unreasonable requests. Indeed, counsel for the business organization should strive to engage the government in dialogue early and often, and to be as transparent as possible in terms of the way it is responding to the government's investigation.

The final step in dealing with the government is typically negotiating a resolution, which can take the form of a monetary payment, a plea agreement, a deferred prosecution or nonprosecution agreement, or a civil corporate integrity agreement or stipulated injunction. While the negotiation of these agreements is beyond the scope of this article, suffice it to say that the facts developed during the internal investigation and disclosed to the government will greatly inform the nature, scope and severity of any settlement.

IV. Conclusion

The COVID pandemic has changed almost every aspect of life, business and culture across the world. Some of these changes, fortunately, will disappear with the emergence of vaccines and the gradual return to normal life, but many others are here to stay. The significantly increased use of telehealth to deliver many basic health care services is one of those developments, and for the most part it is welcome. It will be more convenient for providers and patients and will expand access to those who have difficulty, whether by reason of distance or physical limitations, to visit their providers.

However, as we have demonstrated, there are significant compliance issues with implementing telehealth, either as part of an existing traditional practice or in the emerging industry of telehealth-only providers. From licensing, standard of care, prescribing and privacy through fraud and abuse issues, the issues facing the provision of health care remotely are numerous. And, if something goes wrong—or an allegation is made that something has gone wrong—then a thorough and independent investigation should take place.

[1] *See The Impact of COVID-19 on Outpatient Visits in 2020: Visits Remained Stable, Despite a Late Surge in Cases*, available at https://www.commonwealthfund.org/publications/2021/feb/impact-covid-19-outpatient-visits-2020-visits-stable-despite-late-surge.

[2] *See* Manatt, *Executive Summary: Tracking Telehealth Changes State-by-State in Response to COVID-19*, available at https://www.manatt.com/insights/newsletters/covid-19-update/executive-summary-tracking-telehealth-changes-stat.

[3] *See* AMA, *Telehealth up 53%, growing faster than any other place of care*, May 29, 2019, available at https://www.ama-assn.org/practice-management/digital/telehealth-53-growing-faster-any-other-place-care.

[4] *See* https://www.manatt.com/insights/newsletters/covid-19-update/hhs-renews-covid-19-public-health-emergency-throug.

[5] *See* https://oig.hhs.gov/oas/reports/region5/51600058.pdf.

[6] *See Federal Indictments & Law Enforcement Actions in One of the Largest Healthcare Fraud Schemes Involving Telemedicine and Durable Medical Equipment Marketing Executives Results in Charges Against 24 Individuals Responsible for Over $1.2 Billion in Losses*, available at https://www.justice.gov/opa/pr/federal-indictments-and-law-enforcement-actions-one-largest-health-care-fraud-schemes.

[7] *See* https://oig.hhs.gov/documents/root/230/2020HealthCareTakedown_FactSheet_9dtlhW4.pdf.

[8] https://oig.hhs.gov/reports-and-publications/workplan/summary/wp-summary-0000488.asp.

[9] https://oig.hhs.gov/reports-and-publications/workplan/summary/wp-summary-0000491.asp.

[10] https://oig.hhs.gov/reports-and-publications/workplan/summary/wp-summary-0000535.asp.

[11] https://oig.hhs.gov/reports-and-publications/workplan/summary/wp-summary-0000557.asp.

[12] https://oig.hhs.gov/reports-and-publications/workplan/summary/wp-summary-0000556.asp.

[13] https://oig.hhs.gov/reports-and-publications/workplan/summary/wp-summary-0000397.asp.

[14] *See* https://oig.hhs.gov/documents/speeches/313/hcca-04292021-speech.pdf.

[15] *See Statement of Principal Deputy Inspector General Grimm on Telehealth* by Christi A. Grimm, HHS-OIG Principal Deputy Inspector General, available at https://oig.hhs.gov/coronavirus/letter-grimm-02262021.asp?utm_source=oig-web&utm_medium=oig-whatsnew&utm_campaign=oig-grimm-letter-02262021.

[16] *See* Wall Street Journal, *Calls Grow to Abandon Regulations Eased Under Covid*, April 6, 2021.

[17] *See, e.g.*, Medicare Payment Advisory Commission, *Report to the Congress Medicare Payment Policy*, March 2021 at 469 ("After the PHE ends, providers should no longer be permitted to reduce or waive cost sharing for telehealth services.").

[18] Among sources for developments in telehealth regulation are publications of the American Telehealth Association (https://www.americantelemed.org/press-releases/policyhalftimereport/), the Center for Connected Health Policy (https://www.cchpca.org/resources/state-telehealth-laws-and-reimbursement-policies-report-spring-2021/) and Manatt Health (https://www.manatt.com/insights/newsletters/covid-19-update/executive-summary-tracking-telehealth-changes-stat).

[19] *E.g.*, S.C. Code Ann. § 40-47-37(C)(9).

[20] *E.g.*, Wyo. Rules and Regulations § 052.0001.1 § 7(a).

[21] *E.g.*, Kan. Admin. Reg. § 100-26-1.

[22] *E.g.*, Ariz. Rev. Stat. § 36-3606; N.M. Admin. Code § 16.10.2.11.

[23] *E.g.*, Fl. Stat. Ann. § 456.47 (applies to physician, podiatrist, optometrist, nurse, nurse practitioner, pharmacist, dentist, chiropractor, acupuncturist, midwife, speech-language pathologist, audiologist, occupational therapist, radiological personnel, respiratory therapist, dietician, athletic trainer, orthotist, pedorthist, prosthetist, electrologist, massage therapist, medical physicist, optician, hearing aid specialist, physical therapist, psychologist, clinical social worker, mental health counselor, psychotherapist, marriage and family therapist, behavior analyst, basic or advanced life support service, or air ambulance service, or an individual licensed under a multistate health care licensure compact of which Florida is a member state or an individual who obtains an out-of-state telehealth registration in Florida.); Ariz. Rev. Stat. § 36-3601(2) (applies to podiatrist, doctor of medicine, doctor of naturopathic medicine, nurse, doctor of osteopathy, pharmacist, psychologist, physician assistant, radiologic technologist, doctor of homeopathy or behavioral health professional).

[24] *E.g.*, 02-373 Code of Maine Rules Ch. 6, § 2.

[25] *See* https://www.imlcc.org/.

[26] *See* https://www.nursecompact.com/index.htm.

[27] *See* http://ptcompact.org/.

[28] *See* https://www.emscompact.gov/.

[29] *See* https://aslpcompact.com/ (not yet operational).

[30] *See* https://psypact.site-ym.com/.

[31] It should be noted that a committee of the Uniform Law Commission, the Drafting Committee on Telehealth, is working on a uniform telehealth act, which may include a registration-based model that would allow out-of-state providers to practice in a different state through a registration process (less intense than licensure) to see patients with whom they have an existing relationship, so long as they don't open an in-state office. *See* https://www.uniformlaws.org/viewdocument/2021-april-30-video-committee-meeti-1?CommunityKey=44fb214b-abb6-4d45-8d03-02824bb1c856&tab=librarydocuments.

[32] *See, e.g.*, California Medical Board, *Practicing Medicine Through Telehealth Technology* ("The standard of care is the same whether the patient is seen in-person, through telehealth or other methods of electronically enabled healthcare."), available at https://www.mbc.ca.gov/Licensees/Telehealth.aspx; Idaho Board of Medicine, *Guidelines for Appropriate Regulation of Telemedicine* ("Treatment and consultation recommendations made in an online setting, including issuing a prescription via electronic means, will be held to the same standards of appropriate practice as those in traditional (encounter in person) settings."), available at https://isb.idaho.gov/wp-content/uploads/150402_hea_materials4.pdf. Relatedly, departure from the standard of care can, of course, provide the basis for a professional negligence (malpractice) claim. As with the standard of care, this will be a state law determination, and a review of differing standards for tort liability among the various states is beyond the scope of this article.

[33] *See, e.g.*, Cal. Business & Professions Code § 2290.5 ("Before the delivery of healthcare via telehealth, the healthcare provider initiating the use of telehealth shall inform the patient about the use of telehealth and obtain verbal or written consent from the patient for the use of telehealth as an acceptable mode of delivering healthcare services and public health. The consent shall be documented."); W.Va. Code § 30-3-13a(d)(6) (physician or podiatrist using telemedicine technologies to practice medicine or podiatry shall "obtain from the patient appropriate consent for the use of telemedicine technologies").

[34] Cal. Bus. & Prof. Code § 2242. *Id.*

[35] Florida Statutes Section § 456.47(2)(c).

[36] *See, e.g.*, Cal. Bus. & Prof. Code § 2242.1; N.J. Admin. Code § 13:35-6B.6.

[37] 21 C.F.R. § 1306.03(a). State laws also specifically address controlled substance prescribing, e.g., California Uniform Controlled Substances Act, Cal. Health & Safety Code 11000 *et seq.*; New York State Controlled Substances Act, New York Pub. Health Law Article 3300.

[38] *E.g.*, Cal. Health & Safety Code § 11162.1.

[39] *E.g.*, NYCRR § 80.67.

[40] *E.g.*, Cal. Health & Safety Code § 11165.4(a)(1)(A)(i); N.Y. Public Health Law § 3343-a.2.

[41] The exceptions include, among others, that the patient is in a hospital or clinic registered with the DEA, in the physical presence of a practitioner, and others that do not include a situation in which the patient is at home and the physician sees the patient remotely via telehealth technology. *See* 21 U.S.C. 802(54). The exceptions do facilitate the use of telemedicine for medication assisted treatment of opioid addition; see Drug Enforcement Administration, *Use of Telemedicine While Providing Medication Assisted Treatment (MAT)*, available at https://www.samhsa.gov/sites/default/files/programs_campaigns/medication_assisted/telemedicine-dea-guidance.pdf.

[42] As of March 16, 2020, and continuing for as long as the HHS Secretary's designation of a public health emergency remains in effect, DEA-registered practitioners in all areas of the United States may issue prescriptions for all schedule II–V controlled substances to patients for whom they have not conducted an in-person medical evaluation, provided all of the following conditions are met: the prescription is issued for a legitimate medical purpose by a practitioner acting in the usual course of his/her professional practice; the telemedicine communication is conducted using an audiovisual, real-time, two-way interactive communication system; and the practitioner is acting in accordance with applicable federal and state laws. *See* DEA COVID-19 Information Page (https://www.deadiversion.usdoj.gov/coronavirus.html).

[43] The Ryan Haight Act includes a requirement that any person who operates a website that fits within the definition of an "online pharmacy" must obtain from DEA a modification of its DEA pharmacy registration that expressly authorizes such online activity, and only DEA-registered pharmacies are eligible under the act to obtain such a modification of registration. The act prohibits all controlled substance activities by "online pharmacies" except those expressly authorized by the act. A consequence of this requirement is that non-DEA-registered pharmacies are prohibited from operating online pharmacies. A pharmacy that has obtained such a modification of its registration may not operate as an online pharmacy unless it has notified DEA of its intent to do so and its website contains certain declarations designed to provide clear assurance that it is operating legitimately and in conformity with the act. *See* https://www.deadiversion.usdoj.gov/fed_regs/rules/2020/fr0930_2.htm.

[44] *E.g.*, Cal. Health & Safety Code §§ 11000 *et seq.*; Wash. Rev. Code 69.50 *et seq.*; New York Pub. Health Law, Ch. 45, Art. 33.

[45] *E.g.*, La. Admin Code, tit. 46, Pt XLV, § 7513.C.3; W. Va. Code § 30-3-13a(g)(1); Ohio Admin. Code § 4731-11-09(A), (D).

[46] *E.g.*, Nevada (N.R.S. § 639.23535); Pennsylvania (35 Penn. Stat. § 780-111); California (Business and Professions Code § 688, effective Jan. 1, 2022).

[47] 42 C.F.R. § 423.160(a)(5). Compliance actions against those not in compliance with this requirement will commence January 1, 2022. *Id.*

[48] Cal. Business & Professions Code § 4170 (dangerous drugs); Arizona Rev. Statutes 32-1491; (Rev. Code Wash. 69.50.308(j) (controlled substances); Cal. Health & Safety Code § 11154(a) (controlled substances).

[49] *E.g.*, Arizona Rev. Statutes § 32-1961.01.

[50] *E.g.*, California (Bus. & Prof. Code § 4112); Iowa (I.C.A. § 155A.13A).

[51] *E.g.*, Kentucky Rev. Stat. § 315.0351(1)(g).

[52] 42 U.S.C. 263a.

[53] 42 U.S.C. § 263a(p); 42 C.F.R. § 493.553.

[54] *See* CMS, List of Exempt States Under the Clinical Laboratory Improvement Amendments (https://www.cms.gov/Regulations-and-Guidance/Legislation/CLIA/Downloads/ExemptStatesList.pdf).

[55] *See* https://www.cms.gov/Regulations-and-Guidance/Legislation/CLIA/Downloads/CLIASA.pdf.

[56] *See* CMS, Direct Access Testing (DAT) and the Clinical Laboratory Improvement Amendments (CLIA) Regulations (https://www.cms.gov/Regulations-and-Guidance/Legislation/CLIA/Downloads/directaccesstestingpdf.pdf) ("CLIA authorizes regulation of laboratories that conduct testing, not the individuals who order the tests or receive test results."

[57] https://www.aacc.org/cln/articles/2020/march/direct-access-testing.

[58] 45 C.F.R., Subchapter C.

[59] *See* 45 C.F.R. § 164.308(a)(1).

[60] 45 C.F.R. § 160.203(b); 45 C.F.R. § 164.520(b)(1)(ii)(C).

[61] *See* https://gdpr-info.eu/.

[62] 42 U.S.C. § 12101 *et seq.*

[63] 42 U.S.C. § 12181(7)(F) (including within the definition of "public accommodation with respect to which the ADA applies" "a … pharmacy, … professional office of a health care provider, hospital, or other service").

[64] 42 U.S.C. 18116.

[65] 45 C.F.R. § 92.1 *et seq.* (prohibiting discrimination under, inter alia, any health program or activity receiving federal financial assistance on the grounds prohibited under the ADA.

[66] 42 U.S.C. § 12188; 42 U.S.C. § 2000a-3; 28 C.F.R. § 36.501.

[67] 42 C.F.R. § 482.22(a)(3):

"When telemedicine services are furnished to the hospital's patients through an agreement with a distant-site hospital, the governing body of the hospital whose patients are receiving the telemedicine services may choose, in lieu of the [Medicare rule credentialing requirements], to have its medical staff rely upon the credentialing and privileging decisions made by the distant-site hospital when making recommendations on privileges for the individual distant-site physicians and practitioners providing such services, if the hospital's governing body ensures, through its written agreement with the distant-site hospital, that all of the following provisions are met:

(i) The distant-site hospital providing the telemedicine services is a Medicare-participating hospital.

(ii) The individual distant-site physician or practitioner is privileged at the distant-site hospital providing the telemedicine services, which provides a current list of the distant-site physician's or practitioner's privileges at the distant-site hospital.

(iii) The individual distant-site physician or practitioner holds a license issued or recognized by the State in which the hospital whose patients are receiving the telemedicine services is located.

(iv) With respect to a distant-site physician or practitioner, who holds current privileges at the hospital whose patients are receiving the telemedicine services, the hospital has evidence of an internal review of the distant-site physician's or practitioner's performance of these privileges and sends the distant-site hospital such performance information for use in the periodic appraisal of the distant-site physician or practitioner. At a minimum, this information must include all adverse events that result from the telemedicine services provided by the distant-site physician or practitioner to the hospital's patients and all complaints the hospital has received about the distant-site physician or practitioner."

[68] 42 C.F.R. § 482.22(a)(4):

"When telemedicine services are furnished to the hospital's patients through an agreement with a distant-site telemedicine entity, the governing body of the hospital whose patients are receiving the telemedicine services may choose, in lieu of the [Medicare rule credentialing requirements], to have its medical staff rely upon the credentialing and privileging decisions made by the distant-site telemedicine entity when making recommendations on privileges for the individual distant-site physicians and practitioners providing such services, if the hospital's governing body ensures, through its written agreement with the distant-site telemedicine entity, that the distant-site telemedicine entity furnishes services that, in accordance with § 482.12(e), permit the hospital to comply with all applicable conditions of participation for the contracted services. The hospital's governing body must also ensure, through its written agreement with the distant-site telemedicine entity, that all of the following provisions are met:

(i) The distant-site telemedicine entity's medical staff credentialing and privileging process and standards at least meet the standards at § 482.12(a)(1) through (a)(7) and § 482.22(a)(1) through (a)(2).

(ii) The individual distant-site physician or practitioner is privileged at the distant-site telemedicine entity providing the telemedicine services, which provides the hospital with a current list of the distant-site physician's or practitioner's privileges at the distant-site telemedicine entity.

(iii) The individual distant-site physician or practitioner holds a license issued or recognized by the State in which the hospital whose patients are receiving such telemedicine services is located.

(iv) With respect to a distant-site physician or practitioner, who holds current privileges at the hospital whose patients are receiving the telemedicine services, the hospital has evidence of an internal review of the distant-site physician's or practitioner's performance of these privileges and sends the distant-site telemedicine entity such performance information for use in the periodic appraisal of the distant-site physician or practitioner. At a minimum, this information must include all adverse events that result from the telemedicine services provided by the distant-site physician or practitioner to the hospital's patients, and all complaints the hospital has received about the distant-site physician or practitioner."

[69] *See* TJC Accreditation Manual for Hospitals, July 1, 2021, MS.13.01.01 and MS.13.01/03.

[70] *See* 42 U.S.C. § 1320a-7b(b).

[71] *See* 42 C.F.R. 1003.102(b)(13).

[72] *E.g.*, Cal. Business & Prof. Code § 650.

[73] *E.g.*, Col. Rev. Stat. § 24-31-809; W.Va. Code § 9-7-5.

[74] 42 U.S.C. § 1395nn. Designated health services include clinical laboratory services; physical therapy, occupational therapy and outpatient speech-language pathology services; radiology and certain other imaging services; radiation therapy services and supplies; DME 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.

[75] *E.g.*, Cal. Business & Professions Code § 650.01; Oh. Rev. Code §§ 4731.65-71.

[76] 42 U.S.C. § 1320a–7a(a)(5).

[77] 42 C.F.R. § 1003.1010.

[78] 42 C.F.R. § 1003.110 (definition of "remuneration").

[79] *Id.*

[80] 31 U.S.C. §§ 3729-3733.

[81] The per claim civil penalty is "not less than $5,000 and not more than $10,000, as adjusted by the Federal Civil Penalties Inflation Adjustment Act of 1990 (28 U.S.C. 2461 ... Public Law 104–410." 31 U.S.C. § 3729(a)(1). For civil penalties assessed after June 19, 2020, the range per claim is $11,665 to $23,331. 85 Fed. Reg. 37004, 37006 (DOJ Final Rule, 6/19/2020).

[82] *E.g.*, Cal. Government Code §§ 12650 *et seq.*; New York State Finance Law Section §§ 187 *et seq.*

[83] *See generally Examining Fee Splitting Statutes in the Context of Value-Based Healthcare*, Manatt Health Update, June 22, 2015, available at https://www.manatt.com/insights/newsletters/health-update/examining-fee-splitting-statutes-in-the-context-of.

[84] 42 C.F.R. § 410.78(b)(4).

[85] 42 C.F.R. § 410.78(b)(3).

[86] Cal. Welfare & Institutions Code § 14132.72(e).

[87] 42 C.F.R. § 410.78(b)(2).

[88] *See* Cal. Welfare & Institutions Code § 14132.72 and California Business & Professions Code § 2290.5(a)(3).

[89] *See* https://www.cms.gov/Medicare/Medicare-General-Information/Telehealth/Telehealth-Codes.

[90] *See* 85 Fed. Reg. 84532 (Dec. 28, 2020).

[91] *See* Cal. Business & Professions Code § 2400.

[92] *See* N.Y. State Department of Education, Memorandum to the Members of the Board of Regents, "Corporate Practice of the Professions," June 26, 1998 ("it is clear that business corporations cannot hire a licensee to provide professional services because the law neither authorizes such action nor provides an exemption.") (http://www.op.nysed.gov/corp/corppractice.htm#).

[93] For example, decisions and activities such as scheduling, contracting, setting rates, and hiring and management of nonclinical personnel may implicate CPOM restrictions. *See, e.g.*, 92 Ops.Cal.Atty.Gen. 56 (2009); "A.G. Schneiderman Announces Settlement With Aspen Dental Management That Bars Company From Making Decisions About Patient Care In New York Clinics," available at https://ag.ny.gov/press-release/2015/ag-schneiderman-announces-settlement-aspen-dental-management-bars-company-making.

[94] *See, e.g.*, California Health & Safety Code § 1345(f) (Health care service plan (i.e., regulated entity) is "any person who undertakes to arrange for the provision of healthcare services to subscribers or enrollees, or to pay for or to reimburse any part of the cost for those services, in return for a prepaid or periodic charge paid by or on behalf of the subscribers or enrollees.").

[95] *See, e.g.*, Idaho Statutes § 39-9201 *et seq.*; Montana Senate Bill 101 (effective October 1, 2021); Utah Code § 31A-4-106.5; Rev. Code Wash. § 48.150.060.

[96] *See* Ore. Rev. Stat. § 735.500.

[97] United States Sentencing Guidelines (USSG), § 8B2.1, available at https://guidelines.ussc.gov/gl/%C2%A78B2.1.

[98] https://oig.hhs.gov/compliance/compliance-guidance/index.asp.

[99] *New York Cent. & Hudson River R.R. Co. v. United States*, 212 U.S. 481, 493 (1909); *United States v. Singh*, 518 F.3d 236, 249–50 (4th Cir. 2008); *United States v. Potter*, 463 F.3d 9, 25 (1st Cir. 2006); *United States v. Jorgensen*, 144 F.3d 550, 560 (8th Cir. 1998); *United States v. Sun-Diamond Growers*, 138 F.3d 961, 970 (D.C. Cir. 1998), *aff'd*, 526 U.S. 398 (1999).

[100] While outside the scope of this article, the U.S. Department of Justice has developed a series of factors, commonly called the McNulty/Filip factors, to guide the exercise of this wide prosecutorial discretion in deciding whether to charge corporations and what type of resolution to seek, whether pre- or post-indictment. *See* https://www.justice.gov/jm/jm-9-28000-principles-federal-prosecution-business-organizations#9-28.300.

[101] USSG §§ 8B2.1, 8C2.5(f) and 8C2.8(11).

[102] https://www.justice.gov/jm/jm-9-28000-principles-federal-prosecution-business-organizations.

[103] https://www.justice.gov/criminal-fraud/page/file/937501/download.

[104] While not stated explicitly, there is a sense that the Yates memo emerged as a result of criticism of the Obama-era DOJ for not holding individuals to account for the 2008–09 financial crisis.

[105] Indeed, outside auditors will often engage in a deep review of the internal investigation, starting with the qualifications and experience of the investigative team, moving to the email collection and review, and finally to a review of the facts developed and conclusions reached.

[106] *See, e.g.*, *United States v. Credit Suisse AG*, Crim. No. 1:14-CR-188 (EDVA, 5/19/2014) (Swiss bank's failure to interview key witnesses and preserve documents after being put on notice of a variety of investigations into the use of foreign banks by U.S. citizens to escape tax obligations resulted in denial of cooperation credit and guilty plea). Plea agreement available at https://www.justice.gov/iso/opa/resources/6862014519191516948022.pdf and agreed statement of facts at https://www.justice.gov/iso/opa/resources/3852014519191527936665.pdf.

[107] 18 U.S.C. § 1519 (knowing destruction of documents with intent to impede any federal investigation is a felony).

[108] The review process should include an identification of key issues that the documents relate to and should flag any key or "hot" documents.

[109] *Upjohn Co. v. United States*, 449 U.S. 383 (1981).

[110] The *Upjohn* warnings or admonitions are typically delivered verbally and then documented consistently in the MOI.

[111] If the witness has or is likely to retain counsel, an exception should be noted for discussions with counsel.

[112] The government has made clear that by seeking a waiver of the attorney-client privilege, the government is only seeking **facts** from the business organization, and not legal advice that may have been provided. Justice Manual at § 9-28.710.

[113] In May 2019, the government reinforced these principles in guidance issued to DOJ components handling False Claims Act investigations and proceedings. Justice Manual § 4-4.112.

manatt

Albany
Boston
Chicago
Los Angeles
New York
Orange County
Palo Alto
Sacramento
San Francisco
Washington, D.C.