TRAPS FOR THE UNWARY TELEHEALTH PROVIDER

BY
CAROL K. LUCAS

&
JENNIFER M. GUERRERO

Carol Lucas and Jennifer Guerrero are attorneys in the Health Care Practice Group of Buchalter, a Professional Corporation, resident in the Los Angeles office. Ms. Lucas chairs the Group and has over thirty years' experience representing providers in a range of transactional matters. In addition to assisting clients in health care transactional matters, Ms. Guerrero is an expert in data privacy and cybersecurity.

TechREG CHRONICLE
SEPTEMBER 2022

Visit **www.competitionpolicyinternational.com** for access to these articles and more!

TRAPS FOR THE UNWARY TELEHEALTH PROVIDER

By Carol K. Lucas & Jennifer M. Guerrero

The provision of health care services via telemedicine has been growing in popularity over the last several years. With the arrival of the COVID-19 pandemic, healthcare providers were able to rely on a variety of temporary waivers, executive orders, enforcement discretion and regulations that made the transition to digital healthcare technologies simpler than it had been in earlier times. The use of digital healthcare technologies is now deeply embedded into healthcare services and will continue despite the expiration of the regulatory flexibility afforded by the public health emergency. It is important to remember, though, that health care is largely regulated on a state-by-state basis, and a business structure or payment arrangement that is legal in one state may not readily translate to another state. As the present PHE begins to wind down, providers need to be prepared to face the additional legal and regulatory issues combined with the heightened attention of federal and state authorities to services delivered via telehealth. This article provides an overview of the legislative and regulatory challenges related to the implementation of digital healthcare delivery systems in the United States.

U.S. health care providers are heavily regulated by an overlapping patchwork of laws, including some national law and fifty different state laws. Technology has always outrun the legal framework as providers seek to establish a digital healthcare practice. This complex web of overlapping and sometimes inconsistent laws makes establishing a multi-state medical practice challenging. During the COVID-19 public health emergency ("PHE"), providers and clinicians were able to rely on a variety of temporary waivers, executive orders, enforcement discretion and regulations that made the transition to digital healthcare technologies simpler. As the present PHE begins to wind down, providers must prepare to face additional legal and regulatory issues compounding the already complex regulatory framework that telemedicine providers face.

Even before COVID-19, an increasing number of health care providers were exploring telemedicine, either as an adjunct to their primary brick and mortar practices or as a separate and new venture. The dislocations of COVID-19 accelerated this trend, especially because a number of legal restrictions on the delivery of care via telemedicine were relaxed in connection with the exigencies of the pandemic. Meanwhile, more and more providers have determined that many aspects of the service they provide can be effectively provided remotely if the technology and the tools are adequate.

However, when a provider expands from single-state practice to potentially fifty state practice (or even global practice), the legal and regulatory regime that the provider is used to may not translate to all of the provider's new practice locations. In fact, it almost certainly will not, and telehealth providers need to review a number of different regulatory regimes in each state they propose to practice in. This article will provide insight on multi-faceted digital health regulation to introduce providers and tech entrepreneurs alike to the critical issues they must confront to implement a successful multi-state telemedicine practice.

01
GOVERNMENT ATTENTION TO TELEMEDICINE FRAUD

Meanwhile, possibly because of the exploding popularity of telehealth services, the federal government has turned its attention to telemedicine fraud. On July 20, 2022, the Department of Health and Human Services Office of Inspector General ("OIG") released a Special Fraud Alert warning health care practitioners to exercise caution when entering into arrangements with "purported" telemedicine companies. According to the OIG, unscrupulous telemedicine companies are using kickbacks to reward practitioners for ordering or prescribing medically unnecessary items or services for patients that the provider never examined or meaningfully assessed. Such practices, per the OIG, potentially violate the federal anti-kickback statute, and may also corrupt medical decision-making, drive inappropriate utilization and result in patient harm.

The special Fraud Alert identified a list of suspect characteristics related to practitioner arrangements with telemedicine companies that could present a heightened risk of fraud and abuse. They include:

- The purported patient was recruited by the telemedicine company or its sales agents advertising free or low out-of-pocket cost items or services;
- The practitioner has insufficient contact with or information from the patient to meaningfully assess the medical necessity of the items or services ordered or prescribed; frequently, the provider does not have a medical record but only a questionnaire;
- The practitioner is compensated based on the volume of items or services ordered or prescribed (or the number of records reviewed);
- The telemedicine business only furnishes items or services to federal health care program beneficiaries and does not accept any other insurance;
- The telemedicine company claims not to serve federal health care program beneficiaries, but may, in fact, bill federal health care programs;
- The telemedicine company only furnishes one product or a single class of products, potentially restricting a practitioner's treatment options to a predetermined course of treatment; and
- The telemedicine company does not expect practitioners to follow up with purported patients.

The Special Fraud Alert was careful to note that these factors do not necessarily connote fraud, but were intended to serve a warning that practitioners should be wary of being used by questionable telemedicine businesses. None of this should be surprising to health care providers; paying for referrals or charging for services that were ether not provided or not necessary has always been considered healthcare fraud. What is new is the extra dimension added by purely virtual services and the involvement of the telemedicine company that may not understand a provider's professional requirements, or that may not appreciate how different health care is from other technology-enabled industries.

02
DATA PRIVACY AND CYBERSECURITY

Telehealth providers are bound by federal and state regulations when providing services, just as they would be when providing in-person services. The additional element of providing "remote" care inherently poses risks of unlawful disclosure since it is dependent on the digital infrastructure, which, most often is developed and controlled by a third party that will not guarantee compliance in terms of design, functionality or security. Ironically, the same connectivity provided by telemedicine creates a slew of privacy and security risks, as any data transferred over the internet runs the risk of interception by hackers and other bad actors. While many software programs or platforms purport to comply with Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), there is not a single standard that would certify that the software program or platforms meets all federal and state regulations. Telehealth providers must be aware of the myriad federal and state regulations relating to administrative, physical, and technical safeguards and required notifications, consents and data sharing agreements that may be required to launch a telemedicine practice.

> ***"Telehealth providers are bound by federal and state regulations when providing services, just as they would be when providing in-person services***

HIPAA. The main federal law that governs the collection and use of patient/consumer health information is HIPAA. The U.S. Department of Health and Human Services ("HHS") published what are commonly known as the HIPAA Privacy Rule and the HIPAA Security Rule. The Privacy Rule, or Standards for Privacy of Individually Identifiable Health Information, establishes national standards for the protection of certain health information. The Security Standards for the Protection of Electronic Protected Health Information (the Security Rule) establish a national set of security standards for protecting certain health information that is held or transferred in electronic form. The Security Rule operationalizes the protections contained in the Privacy Rule by addressing the technical and non-technical safeguards that organizations called "covered entities" must put in place to secure individuals' "electronic protected health information" ("e-PHI").

Telehealth providers should be familiar with HIPAA and its privacy and security requirements as it not only applies to telemedicine, but to any traditional medical practice that transmits health information in electronic form. However, since HIPAA only applies to individuals and entities who qualify as a covered entity or a business associate, and not necessarily all third party vendors, many technology partners are ignorant to its requirements. Since HIPAA is not applicable to these technology partners, the software platform or mobile application may not incorporate all the required administrative, technical, and physical safeguards. Likewise, if they use other vendors (cloud service providers, help desk, etc.), chances are such vendors are not compliant either. Further, HIPAA does not directly apply to many consumer-based digital health software or applications. For example, information (including medical information) provided by a consumer to a medical device or other company that is not a covered entity or business associate is not required to comply with HIPAA.

This gap in coverage places the burden on the telehealth providers to ensure their own compliance and their vendor's compliance (including subcontractors) with HIPAA through their third-party contracts (commonly called business associate agreements or "BAAs"). Telehealth providers can review the HHS Health Industry Cybersecurity Practices ("HICP"): Managing Threads and Protecting Patients, for practical guidelines to manage cyber threats and protect patients.

State Privacy Law Considerations. In addition to HIPAA, telehealth providers must take into account numerous state privacy laws when establishing a national telehealth practice. While some state laws are duplicative of the requirements under HIPAA, a number of state laws impose more stringent requirements that impact consumer/patient consent and notice requirements, employee training requirements, patient records request and other privacy requirements. For example, under California law a patient authorization is not HIPAA-compliant unless it is in fourteen point font. In Texas, a covered entity only has fifteen days from the patient's request to produce electronic copies of their electronic health record, reducing the timeframe of thirty days under HIPAA. Similarly, other state laws are potentially triggered based upon the type of information a company collects and uses. If genetic data is collected, states like California, Wyoming, and Utah impose additional notice and consent requirements. Both Illinois and Texas impose additional regulations on companies who collect and use biometric identifiers.

To make things more complicated, a number of states, including California, Utah, Colorado, Virginia, and Connecticut, have passed comprehensive privacy laws that impact the delivery of telemedicine services, notice requirements (privacy policies), consent requirements from consumers not only subscribing to the telehealth services but also those browsing telehealth provider's

websites, and data breach notification requirements. The misconception that these laws are inapplicable is a fatal mistake, since most telehealth providers engage in some form of e-commerce and collect consumer data of non-patients that is governed by state law rather than HIPAA.

PCI Compliance. Telehealth providers that store, process, or transmit credit card data are required to adhere to the same standards as a business in any other industry. Typically, a brick and mortar provider may have implemented a payment system that did not require them to store, process, or transmit credit card data. However, with the rise of technology and e-commerce, most providers are at minimum transmitting credit card data to a third party provider, like Stripe or Clover.

If a provider stores, processes, or transmits credit card data, it must maintain Payment Card Industry ("PCI") compliance to ensure that all transactions using credit or debit cards are safe and secure in order to protect the patients and the provider from unauthorized access. While there are many overlapping security measures between PCI compliance and HIPAA, telehealth providers still need to undergo an annual PCI compliance audit. Telehealth providers that utilize third party payment processors should also ensure that their vendor is PCI Compliant.

Cybersecurity Insurance. Cybersecurity insurance can help hedge the costs of a cyber-security incident or data breach. In some cases, liability insurance may cover telehealth services, but may carve out costs related to a cyber-security incident or data breach. Before procuring any insurance, telehealth providers should review the coverage limitations.

03

TECHNOLOGY REGULATION AND ADVERTISING ISSUES

The U.S. Food and Drug Administration ("FDA") regulates many types of digital health technologies that are considered "medical devices" such as mobile health/medical applications and software, health information technology, wearable devices, telehealth, and telemedicine. Interestingly, the FDA expands the definition of telemedicine to include the delivery of medical information or counseling to patients over the phone, including the use of home specimen collection kits where the distributors deliver the results of the test and counseling to the consumer via phone or technology platform purporting to cast a larger net of companies. However, the FDA has stated that it intends to enforce compliance where the medical device poses more than a minimal risk to consumers.

Section 5(a) of the Federal Trade Commission Act ("FTC Act") (15 USC §45) also applies to telehealth providers and prohibits "unfair or deceptive acts or practices in or affecting commerce." Telehealth providers and their vendors are prohibited from making deceptive or misleading claims, and engaging in acts or practices that cause, or are likely to cause, substantial injury to consumers that they cannot avoid and that do more harm than good.

Any developer of` a mobile health app that collects, creates, or shares consumer information, telehealth providers can use the tool on the Federal Trade Commission's website to find out when the FDA, Federal Trade Commission ("FTC"), or HIPAA laws apply.

04

TELEHEALTH CONTRACT ISSUES

Telemedicine providers should be weary of blindly entering into telemedicine contracts with developers (if they are creating their own platform/application), document storage vendors, software and mobile application vendors, and other types of technology agreements. Many of these agreement (if not all) contain one-sided limitation of liability clauses, lack appropriate indemnification and data security provisions, do not appropriately protect the telemedicine provider's intellectual property and/or consumer data, or fail to meet regulatory requirements. Negotiating a fair vendor contract is essential to protecting the telehealth provider's practice from noncompliance and liability.

Limitation of liability clauses should include a value large enough to cover the damages that could be reasonably assumed by the vendor. Carve outs for incidental, consequential, and punitive damages may prevent recovery caused by the vendor's negligence, or any fines or penalties imposed from a data breach of the system. Indemnification should be fair given the scope of services and should work in conjunction with the limitation of liability. Intellectual property indemnification is typically provided by the vendor since the vendor supplies the intellectual property. Data security and privacy provisions for telemedicine services should comply with HIPAA, including the execution of a business associate agreement.

05
LICENSING AND PARITY

Licensing. Licensing can create many issues for telehealth programs. Generally telehealth providers need to be licensed in the states in which the patients are located. A physician physically located in Missouri, for example, could treat a patient located in California if the physician is licensed in California, the state in which the patient resides. Therefore, with limited exceptions, telehealth consultations with a physician across state lines require some form of licensing paperwork depending on rules set by the state where the patient is located.

Interstate compacts (agreements among two or more states) can streamline the process for health care providers to practice in multiple states — expediting the licensing process or allowing members to practice under a single multistate license. These include:

- The Interstate Medical Licensure Compact ("IMLC") streamlines the licensing process for physicians so they can practice medicine in multiple states. About 80 percent of physicians meet the criteria for licensure through the Compact, according to the Interstate Medical Licensure Compact Commission ("IMLCC"). Thirty-nine states have joined the compact.
- The Nurse Licensure Compact ("NLC") authorizes eligible nurses to practice across multiple member states while maintaining a single license.
- The Psychology Interjurisdictional Compact ("PSYPACT") authorizes eligible psychologists to practice telepsychology across member states.
- The PT Compact authorizes eligible physical therapists to work in multiple member states under a single license.

Just as licensure requirements depend on the patient's location, so do regulations governing a provider's mode of practice, including scope of practice issues, supervision requirements and consent requirements. Simply stated, a medical (or other provider) licensed in a particular state carries with him or her that state's regulation of a licensee. For example, a nurse practitioner's scope of independent practice (i.e. what a nurse practitioner may lawfully do without physician supervision) may be vastly different in California than in Arkansas. Even if practitioners obtain their licenses via a single application through a multi-state compact, they are charged with compliance of the laws in each such state.

Parity. The term "parity" means two different things in connection with insurance coverage for telehealth services: coverage parity and payment parity. Coverage parity requires payors to reimburse providers for services provided via telehealth if the same service is covered in person. Payment parity goes a step further and requires payors to reimburse the same amount for a service provided via telehealth means. Approximately 40 states have passed laws mandating coverage parity. Of those, 31 mandate payment parity. Even in states with parity requirements, however, coverage varies. Some laws cover only physician services; others more broadly cover virtual care and remote patient monitoring as well, services that only exist in a telehealth environment.

Additional parity mandates were implemented in response to the COVID-19 pandemic, including coverage for services delivered via telephone and requiring waiver of patient co-payments. It is not clear how long any special pandemic rules will last or the extent to which certain new rules may become permanent.

06
UNIQUE TELEHEALTH LAWS THAT APPLY TO A MULTI-STATE PRACTICE

A comparison of how California and Texas regulate the establishment of a physician-patient relationship is instructive. For California, the physician must conduct an "appropriate" initial examination. Depending on the nature of the service, that examination could be accomplished remotely, but may need to be conducted in person. The California Medical Board leaves that decision to the professional judgment of the physician.

Texas requires physicians to have an established relationship with the patient before prescribing medications via telehealth. Previously, establishment of a relationship required an in-person encounter, although Texas now permits the relationship to be established through a live video telemedicine visit.

Further, the federal Ryan Haight Act requires a controlled substance prescription to be issued by a practitioner who has conducted at least one in-person medical evaluation or by a covering provider if the primary provider is unavailable. This requirement was waived for the duration of the COVID-19 public health emergency, but as of now is set to become effective once again 151 days after the end of the

public health emergency. The public health emergency currently expires on October 13, 2022, but may be extended again.

Corporate Practice of Medicine: The corporate practice of medicine prohibition generally prohibits lay (i.e. non-professional) entities from providing medical services. In most corporate practice states, that means that a general business corporation cannot provide and charge for physician services. A telemedicine provider located in a state without a corporate practice ban may be organized as a general business entity and may employ physicians. Consider this example: Oklahoma is not a corporate practice of medicine state; Texas is a corporate practice state. If a telemedicine provider in Oklahoma were to provide services to a patient in Texas through a Texas-licensed physician employee, the payment by the Texas patient to the telemedicine provider could be held to violate Texas's corporate practice of medicine ban. Further, not all states permit foreign (i.e. sister state) professional entities to practice there. If they do, they generally require local licensure by some or all of the entity's owners, officers and directors or managers. New York, for example, permits the qualification of foreign professional service corporations in New York, provided that all of the shareholders, officers, and directors are licensed to practice medicine in New York.

> ***Further, the federal Ryan Haight Act requires a controlled substance prescription to be issued by a practitioner who has conducted at least one in-person medical evaluation or by a covering provider if the primary provider is unavailable***

Telemedicine provider businesses in corporate practice of medicine states generally adopt a management services organization ("MSO")/friendly professional corporation ("PC") model. Under this model, an MSO, owned wholly or in part by non-licensed individuals, provides administrative support services to a medical practice pursuant to a written services agreement. Often, the MSO provides everything that that does not require a medical license to provide, including space, supplies, equipment, non-professional staff, accounting, billing and collection, and payables management. A well-crafted management services agreement clearly recognizes the PC's control over all clinical decisions and the medical practice itself, including the authority to hire physicians, set clinical protocols and enter into agreements to provide medical services. In the telemedicine context, the MSO is the technology-enabled platform company. There is risk, however, if the MSO fails to observe the professional separateness of the PC or its providers.

Physician Dispensing: If the telehealth provider dispenses medication to patients in remote locations, laws relating to physician dispensing will be implicated. Here again, state laws vary. The New York Board of Pharmacy takes the position that physicians may not dispense in New York at all. In California, physicians may dispense as long as they comply with all statutory requirements regarding labeling, etc. Florida permits physician dispensing upon registration with the Florida medical licensing board as a dispensing practitioner and compliance with pharmacy disclosure regulations.

Language Interpretation Services: Telemedicine providers are subject to the Americans with Disabilities Act ("ADA") and the federal Civil Rights Act. The ADA requires public accommodations to ensure that no individual with a disability (including deafness or hearing impairment) is excluded, denied services, segregated or otherwise treated differently than other individuals because of the absence of auxiliary aids or services. Health care providers are places of public accommodation for purposes of the ADA, which means that telemedicine services for hearing or vision impaired patients should be made available. States also vary widely in requirements to provide services for variously impaired patients. For example, Mississippi requires the telemedicine equipment and network used for remote patient monitoring services to accommodate non-English language options. New York requires culturally competent translation services for telepsychiatry.

The federal Civil Rights Act of 1964 may also apply. The Act prohibits discrimination based on race, color, or national origin, which includes limited English proficiency individuals. The Act applies to entities receiving "federal financial assistance," including Medicare Part A. To the extent that a hospital provides telemedicine services, its remote services, as well as its in-person services, are required to provide language assistance.

For telemedicine providers, licensing laws are only the starting point. Telemedicine providers should be aware that a business model that complies with one state's laws may not be exportable without review and some tweaking.

CPI SUBSCRIPTIONS

CPI reaches more than **35,000 readers** in over **150 countries** every day. Our online library houses over **23,000 papers**, articles and interviews.

Visit **competitionpolicyinternational.com** today to see our available plans and join CPI's global community of antitrust experts.

CPI COMPETITION POLICY™ INTERNATIONAL