2019 Cyber, Management and Professional Liability Conference
July 10-12, 2019
Boston, MA

Telemedicine – the Cryptocurrency of Professional Liability: Trends, Benefits, and Risks

I. Telemedicine Innovation and Regulation

A. Definitions and Examples of Telemedicine

The term "telemedicine" takes on a variety of definitions ranging in the scope of activities, people, and modalities covered. For example, the World Health Organization defines the terms "telehealth" and "telemedicine" interchangeably as, "[t]he delivery of health care services, where distance is a critical factor, by all health care professionals using information and communication technologies for the exchange of valid information for diagnosis, treatment and prevention of disease and injuries, research and evaluation, and for the continuing education of health care providers, all in the interests of advancing the health of individuals and their communities." The American Telemedical Association takes a similar approach, viewing "telemedicine and telehealth to be interchangeable terms, encompassing a wide definition of remote healthcare." Some definitions distinguish telehealth and telemedicine, with the former being used to refer to health care services delivered by all health care providers, and the latter being used to refer only to health care delivered by a physician. Louisiana restricts telemedicine to "the practice of health care delivery, diagnosis, consultation, treatment, and transfer of medical data using interactive telecommunication technology that enables a health care practitioner and a patient at two locations separated by distance to interact." Even stricter is New York's definition of telemedicine as "the delivery of clinical health care services by means of real time two-way electronic audio-visual communications which facilitate the assessment, diagnosis, consultation, treatment, education, care management and self management of a patient's health care while such patient is at the originating site and the health care provider is at a distant site."

In any case, telemedicine should be distinguished from the more general term, "E-Health," which describes a broad range of activities positioned at the intersection of health and technology. The World Health Organization (WHO) defines "E-health" as "the use of information and communication technologies (ICT) for health." While telemedicine is always E-health, E-health is not always telemedicine. The distinction is often not easy to make, but is essential when determining whether a doctor-patient relationship exists through the online interaction between a provider and an E-health consumer.

B. The Doctor-Patient Relationship in Telemedicine

The doctor-patient relationship arises when a physician renders and the patient accepts professional medical services. Historically, physical face-to-face contact anchored the doctor-patient relationship, but E-health has eliminated the element of physicality in many instances. For example, specialists at John Hopkins use webcams to conduct remote visits with nursing home residents hundreds of miles away. The legal obligation that commences with a doctor-patient relationship is a prerequisite to medical malpractice liability. Since the practice of medicine marks an essential component of the doctor-patient relationship, it becomes crucial to distinguish between the practice of medicine and the provision of medical information. In this regard, the differing definitions of the scope of medical practice adopted by different states do little to clarify when provision of online health information crosses into the realm of medical practice.

Telemedicine will only continue to blur the line between medical information and medical practice. For example, it is unclear whether initial interactions between E-health consumers and physicians in an online forum will give rise to a doctor-patient relationship. Although the case law is scarce, there are some decisions that provide guidance for determining when a doctor-patient relationship might arise as a result of E-health activity. First, in cases involving telephonic medical consultations between a doctor and a patient, courts are likely to find a doctor-patient relationship when: (1) the doctor gives affirmative advice regarding a specific course of treatment, (2) it is foreseeable that the patient will rely upon the doctor's advice, and (3) the patient relies upon the doctor's advice. Second, drawing from cases involving the distinction between general investment advice and the professional practice of a securities dealer, U.S. courts have indicated that the provision of medical information would cross into the realm of medical practice when: (1) the doctor and the patient communicate directly, (2) the doctor provides professional advice in response to the patient's particular medical situation, and (3) the encounter resolves the patient's issue without the need to obtain further medical advice. In a rare telemedicine case, one court found that an isolated online psychiatric consultation established a doctor-patient relationship.

C. Telemedicine and Innovation

The integration of technology in health care makes possible everything from scheduling doctors' appointments online to robotic surgery. Telemedicine has the ability to improve health care access and outcomes through the use of live video, mobile health (mHealth), remote patient monitoring, and store-and-forward communications. For example, patients who experience geographic barriers to health care can access doctors remotely using the telephone, computers, or mobile devices. This burgeoning field empowers patients to become active participants in the prevention and management of their medical conditions. Doctors can improve patient care by using E-health modalities to collaborate and consult with one another around the world. Health care organizations can employ telemedicine to expand health care services and reduce costs associated with onsite care that could be provided remotely. In addition to the expansion of human-provided health services, artificial intelligence makes computer-provided health services possible. Dr. A.I., Healthtap's virtual A.I.-powered physician, uses a data repository generated from billions of interactions between patients and doctors, to

"instantaneously translate[] a person's symptoms into personalized, doctor-recommended courses of action."

Providers and patients alike accept high-tech health care. In its 2016 Digital Health Study, the American Medical Association found that most physician respondents recognized the potential for digital tools to improve patient care by enhancing work efficiency, patient safety, and diagnostic abilities. In a 2018 consumer survey on digital health, 56% of American respondents reported using websites and 46% reported using a mobile phone or tablet to manage their health. And technological innovation in health care shows no signs of slowing. The telemedicine market is projected to reach $13 billion dollars by 2020. In addition, 80% of health care executives in the U.S. agree that artificial intelligence will work next to humans within the next two years and 72% agree that extended reality ("technology [that] immerses users in visual, audio, and potentially olfactory and haptic cues") will have a widespread impact on every industry over the next five years, including health care.

D. Regulation of mHealth applications and wearable tech

Telemedicine does not come without its challenges, including an array of implementation cost, privacy, technology, safety, ethical, and legal concerns. One of these legal concerns is whether mobile health (mHealth) applications and wearable technologies are regulated by the FDA as medical devices. According to the Food and Drug Administration, regulated medical devices are, "[h]ealthcare products intended for diagnosis, cure mitigation, treatment, or prevention of a medical condition intended to affect the structure or any function of the body." Mobile applications will be considered regulated medical devices if they manage and transmit patient specific data for a regulated device (i.e. "connectors"), have functionalities similar to regulated devices (i.e. "replicators"), actively monitor patients (i.e. "loggers and trackers") or use patient data to "analyze, diagnose, and/or treat a patient" (i.e. "automators and customizers"). However, the FDA exercises discretion when enforcing regulations for mobile applications that pose a low risk of patient harm, for example, fitness trackers. It should be noted that some legal scholars believe that litigation will play a large role in indirectly regulating mHealth applications and wearable technologies "during a period of light regulation by traditional regulators."

II. Telemedicine Risks and Claims

A. Data and Security in Telemedicine

While mere mention of data and telemedicine together immediately provokes fears related to data security, it should also be noted that data collection in connection with the provision of telemedicine can provide enormous benefits. On an individual level, the collection of health data can help ensure continuity of care, decreasing the risk of medical errors and improving the quality of care. Easy patient access to data also improves transparency and trust between patients and health care providers. On a larger scale, health data aggregation can help reach the goal of high-quality low-cost health care by identifying problem patterns, including potential epidemics, bio-threats, and safety concerns, and enabling statistical analysis of clinical and economic performance.

Of course, the collection and use of health data must be handled carefully. The Health Insurance Portability and Accountability Act of 1996 (HIPAA), which governs the processing of "protected health information" (PHI) in the United States, has a dual goal of improving information access as well as protecting patient privacy. PHI is "any information in a medical record that can be used to identify an individual, and that was created, used, or disclosed in the course of providing a health care service, such as a diagnosis or treatment." HIPAA also defines electronic protected health information (ePHI) as "individually identifiable health information that is created, maintained, or transmitted electronically by mHealth . . . and eHealth products. This includes PHI on desktop, web, mobile, wearable and other technology such as email, text messages, etc." In the telemedical context, an email to a doctor's office requesting a prescription or online appointment scheduling request would be considered PHI while the number of steps recorded on a pedometer, heart rate readings, or number of calories burned without personally identifiable information would not. Any mHealth application or wearable device that stores and transmits the user's personally identifiable information, whether intended or not, to a covered entity must be HIPAA compliant. HIPAA allows the processing of HPI absent patient consent and absent specific use disclosures as long as adequate security is in place. In the event of a data breach, the offending entity must report the breach within 60 days.

Since telemedicine has international reach, it is also important to be aware of the European General Data Protection Regulation (GDPR), which unlike HIPAA, is a patient-centric regulation that covers all European Union residents regardless of where the provider is located. The GDPR regulates "personal data" defined as "any information relating to an identified or identifiable natural person." GDPR regulations for "data concerning health" are more stringent. "Data concerning health" is "personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status." Completely anonymous data is not covered by GDPR, but pseudonymized data is protected under less stringent standards. While a comprehensive analysis of data protection regulations is outside of the scope of this discussion, we highlight some differences between HIPAA and GDPR. Unlike HIPAA, GDPR requires the patient's explicit consent before processing health data. GDPR also requires permissions and disclosures for each data use, with the exception that pseudonymized data can be processed for use beyond the purpose for which the data was originally collected. Under the GDPR, but not HIPAA, patients have a right to erasure. Significantly, in the event of a data breach, GDPR requires notification within 72 hours, while HIPAA demands notification to patient within 60 days.

B. Telemedicine Coverage and Claims

Providers offering telemedical services should confirm adequate insurance coverage. Physicians' professional liability policies may not cover claims related to privacy breaches or products liability that can arise from the use of telemedicine. Many insurers offer additional coverage options for telemedical activities through endorsements or separate telemedicine policies. Insurers offering telemedicine coverage should ensure that providers comply with all applicable state laws and regulations governing telemedicine. They should also confirm that the provider has adequate policies and protocols in place for their telemedicine programs.

Telemedicine claims are relatively new and the case law is limited. The use of telemedicine can give rise to claims for malpractice, products liability, and privacy breaches. Defendants can include health care providers, health care institutions, and software developers. For health care providers, liability may arise in connection with a range of activities, including designing telehealth services and products, using or recommending, or failing to use

telemedicine to provide patient care, or failing to disclose risks of telemedicine. For providers who exercise professional medical judgment in connection with application design, there will likely be no doctor-patient relationship, and therefore, no duty will be imparted should a medical malpractice claim arise. However, the provider may be subject to products liability in connection with application design activities. For providers who recommend or use (or fail to use) telemedicine in the course of treatment, the standard of care, as in all medical malpractice cases, requires reasonable medical judgment. However, it is anticipated that courts will eventually require that providers have knowledge about the operation of telemedical technologies that they employ in the provision of care. We believe that courts will soon ask whether providers knew or should have known about product or design defects of the telemedical technologies they utilize. Currently, lability for failing to disclose risks of telemedicine is analyzed under the standard informed consent rules, which depend upon whether the jurisdiction adheres to a patient-centered risk disclosure standard. Health care institutions may owe direct duties to patients in the selection, deployment, staffing, and updating telemedical technologies in use. Software developers will likely face liability for design defects under products liability rules.

III. Cross-border telemedicine

A. Licensing

"Telemedicine is not a new medical act . . . [rather] it represents an innovative way of providing health care services." As such, telemedicine providers must be aware of state laws and state medical board regulations that generally govern the practice of medicine. As discussed earlier, states define the practice of medicine and telemedicine differently, but the core activities of diagnosis and treatment will generally be considered medical practice. Since the practice of medicine usually occurs where the patient is located at the time of treatment, telemedical providers must comply with licensing requirements in every state where they treat patients. Some states have special telemedical licensing procedures, while others require full medical licensure. In addition, some telemedicine providers will be exempted from licensing requirements in some states pursuant to a "common consultation exception." For example, Louisiana excludes from its definition of telemedicine, "an informal consultation or second opinion, provided by an individual licensed to practice medicine in a state other than Louisiana, provided that the Louisiana physician receiving the opinion is personally responsible to the patient for the primary diagnosis and any testing and treatment provided." Finally, we note that the Interstate Medical Licensure Compact (IMLC), which currently has 24 member states, may help bring consistency to telemedical licensing requirements.

B. Choice of Law and Jurisdiction

Cross-border telemedicine introduces questions about choice-of-law and jurisdiction. A physician who provides treatment to an out-of-state patient likely has sufficient minimum contacts to satisfy due process and confer jurisdiction to courts in the patient's home state. While states take variety of approaches to choice-of-law rules, most adopt the "most significant relationship" test used by the Restatement (Second) Conflicts of Law. In the majority of cases, the law of the place of treatment will govern medical malpractice disputes. It is also widely

accepted that the place of treatment in telemedicine is the place where the patient is located at the time of treatment. However, this becomes more difficult to determine in cases where the provider renders care to the patient in multiple states. When considering choice-of-law issues, one must also be cognizant of the difference between substantive and procedural law. In medical malpractice cases, many procedural laws, such as statute of limitations, have a significant impact on the litigation. It is not always easy to delineate which laws are substantive and which are procedural. For example, statutes of limitations were historically considered procedural, but modern reforms have reclassified them as substantive or subjected them to borrowing statutes that would apply the shorter statute of limitations. Medical malpractice pre-trial screening and arbitration laws will also generally be considered substantive laws subject to a choice-of-law analysis, unless the statute itself limits its application to a particular jurisdiction. For example, Maryland's pre-trial arbitration requirement is specifically limited to lawsuits brought "in any court of th[at] State." In the case of damages caps, the court usually applies the law most favorable to plaintiffs, with the potential exception for claims filed in the defendant's home state when that state's damages rule is more conservative.

Avoiding the default choice-of-law and jurisdiction rules through contractual choice clauses is tempting but may not be valid when one of the contracting parties is the patient. We must consider public policy objectives related to consumer protection since a telemedicine contract is a consumer contract. It is widely recognized that consumers cannot protect their interests as well as their professional contracting partners as a result of "inferior bargaining power." Some scholars argue that patients as consumers are even weaker contracting parties. As a result, many legal systems seek to protect consumers by restricting the freedom of the contracting parties to choose the applicable law. Some jurisdictions, including Oregon and Louisiana, expressly prohibit choice-of-law clauses in consumer contracts, and a federal court sitting it those states will likely invalidate choice-of-law and venue selection clauses in a consumer telemedicine contract as contrary to public policy. Even when a choice-of-law or forum selection clause is not expressly prohibited by law, a court may still find that it violates public policy. Courts usually find a violation of public policy when the chosen law deprives the consumer of protection or a legal remedy available under the law of the consumer's home state.