Advice for telehealth providers with international ambitions

Amy Lerman of Epstein Becker Green's Health Care and Life Sciences practice provides an overview of key legal and regulatory considerations for US healthcare providers seeking to provide telehealth services internationally.

US based telehealth providers not only treat patients in remote or underserved regions, but also can access an international market of patients seeking access to specialty care in the US without having to travel to get it. All indications are that the global healthcare marketplace is ripe with opportunities for US based healthcare providers[1] to deliver high quality healthcare via telehealth technologies to patients worldwide. Yet, with these opportunities come certain challenges. Putting aside potential economic barriers to launching any telehealth initiative, US based healthcare providers seeking to provide international telehealth services face legal and regulatory uncertainties. Most notably, while telehealth technologies have advanced to the point where provision of international telehealth services are possible, the laws in many countries have not kept pace with the technological advances. Rather, most countries regulate the provision of telehealth through existing patchworks of laws and regulations that reflect traditional understandings of healthcare as predominately a local enterprise. As a result, telehealth providers often must contend with countries, and within these countries, states, provinces and municipalities that have differing practice standards, licensure requirements, and systems of accountability. Providers that are bound by US laws and regulations regarding the practice of medicine must balance their domestic practice requirements against any relevant foreign requirements, which in some cases may be competing and/or more onerous.

As a result of this framework, providers seeking to practice telehealth across international borders face significant legal and regulatory questions. In most of the world there are no standards, guidelines, or processes to guide the practice of cross border telehealth. This article offers a preliminary overview of key legal and regulatory considerations for such US providers.

Fraud and abuse laws

The practice of telehealth across international boundaries by US based providers requires vigilance to the US fraud and abuse laws. Concerns in an international telehealth context may relate to the infrastructure, equipment, and personnel needed to provide telehealth services. Moreover, the healthcare industry is taking advantage of lower costs and easily accessible physician services overseas, particularly in disciplines such as radiology. A 'distant' site for telehealth services may receive free or discounted equipment from the 'originating' site or another provider or vendor, or the billing arrangement for telehealth services provided by a physician overseas may complicate existing relationships that are otherwise compliant.

Simply put, all potential telehealth initiatives should be analysed for fraud and abuse risks. Federal fraud and abuse laws (most notably the Anti-Kickback Statute ('AKS')), relevant state fraud and abuse laws, and fraud and abuse compliance guidance by the US Department of Health and Human Services Office of Inspector General[2], should be considered when structuring relationships among healthcare providers that would participate in the provision of international telehealth services. Any proposed arrangement must be analysed from each party's perspective and specific consideration must be given to understanding what benefits either party may receive in return for inducing referrals. Applicable safe harbors should be examined to protect potential telehealth arrangements that would otherwise violate the AKS[3]. Note, however, that safe harbors are remuneration-specific and do not globally protect any potential arrangement.

Licensure

Considerations with regard to licensure include whether a provider's local (state) Board of Medicine has taken a position regarding state licensed physicians who practice medicine internationally, as well as whether telehealth services provided to patients internationally would be considered the 'practice of medicine' by the state in which the provider is licensed. Providers must consider whether, in addition to a local licence, they also would need a separate licence to practice in the foreign jurisdiction(s) where telehealth patients are located, under the relevant foreign law(s). As is the case in the US, foreign countries regulate the practice of medicine via a web of regulatory complexity, often decentralised and highly dependent upon standards of local governance. Many countries do not specifically address the provision of telehealth services, may only address this narrowly, or may simply implicate the practice of telehealth indirectly.

Europe has taken meaningful steps to expand the practice of telehealth across borders by making licensure issues more surmountable. In June 2012, the

European Commission published a 'Commission Staff Working Document on the Applicability of the Existing E.U. Legal Framework to Telehealth Services,'[4] which provides guidance on how to comply with EU laws and highlights where EU and US standards may diverge. Licensing in the EU is similar to the current US system, where each state is responsible for its own licensing requirements and enforcement. However, the EU system differs where cross border provision of care is involved due to the 'country-of-origin principle.'[5] Under this principle, a provider in an EU Member State is 'practicing medicine' legally if they comply with the licensure requirements in that Member State and treats the patient from within their Member State, regardless of whether the patient is located in another Member State and irrespective of the requirements in the other Member State. The 'country-of-origin principle' is the key difference between the US and the EU regarding licensure issues and the exact inverse of how licensure has traditionally worked in the US[6].

Privacy and security

The practice of healthcare today occurs amid active enforcement of the Health Insurance Portability and Accountability Act of 1996 ('HIPAA') privacy and security laws and regulations[7]. By virtue of providing services within US boundaries, healthcare providers have developed policies, procedures, and systems to ensure the privacy and security of patients' protected health information ('PHI'). The same caution is worthwhile when US healthcare providers seek to transfer PHI between the US and foreign countries. Provider policies must strike the right balance between protecting PHI in the normal course of providing services generally and protecting PHI in instances that may uniquely arise in the context of providing international telemedicine services, particularly where information is shared with foreign based entities and there is potential for such information to be improperly shared by the foreign entity. At least four potentially relevant sources of legal authority should be considered: (1) federal requirements under HIPAA, (2) relevant state privacy and security laws, (3) privacy and security laws in the foreign countries where telehealth services are provided, and (4) any contractual obligations between the US and foreign providers sharing the information. Business Associate agreements should be in place with international providers and even vendors of telehealth technologies, as appropriate.

US healthcare providers seeking to access the international telehealth market must carefully assess the legal and regulatory requirements, and limitations, of any potential international telehealth arrangement.

Foreign Corrupt Practices Act 1977 ('FCPA')

The provision of international telehealth services can also expose US healthcare providers to heightened risks under laws such as the FCPA, an anti-bribery law intended to eliminate the practice of paying a 'foreign official' for the purpose of obtaining or retaining business[8]. The term 'foreign official' has been interpreted broadly and, in the context of healthcare, potentially includes anyone who works for a government owned or operated healthcare system, including those who may be primary points of contact when developing international telehealth initiatives. Given the severity of potential FCPA penalties, providers contemplating international telehealth initiatives should consider developing and implementing education and training programs focused on compliance with the FCPA.

Conclusion

US healthcare providers seeking to access the international telehealth market must carefully assess the legal and regulatory requirements, and limitations, of any potential international telehealth arrangement. This requires analysis of local laws, customs, and standards of practice in each of the countries where telehealth services would be provided.

Amy Lerman Associate
Epstein Becker Green, Washington DC
alerman@ebglaw.com

1. References throughout this article to 'providers' are intended as references to both individual practitioners as well as healthcare entities.
2. This is the agency responsible for enforcing the AKS; it has published three noteworthy Advisory Opinions addressing telehealth-related fraud issues. The most recent Advisory Opinion, issued in 2011, lays out a helpful fact pattern for providers considering how to structure arrangements through which telehealth services would be provided. OIG Adv. Op. No. 11-12 (Aug. 29, 2011).
3. 42 C.F.R. § 1001.952.
4. European Commission, 'Commission Staff Working Document on the Applicability of the Existing E.U. Legal Framework to Telehealth Services' (June 12, 2012).
5. The 'country-of-origin principle' is a component of the eCommerce Directive, enacted by the EU in 2000 to set up an internal market framework for electronic commerce and to provide legal certainty for businesses and consumers.
6. Recent developments, notably the Federation of State Medical Boards' draft Interstate Medical Licensure Compact ('FSMB Compact'), may bring the US licensure system more in line with the EU system. The FSMB Compact is designed to facilitate physician licensure portability and practice of interstate telehealth by streamlining the licensure process through the creation of an additional licensure pathway through which physicians could obtain expedited licensure in participating states.
7. 45 C.F.R. Parts 160 and 164. The primary enforcement body for HIPAA laws is the US Department of Health and Human Services Office of Civil Rights.
8.15 U.S.C. § 78dd-1 et seq.