Volume 7, Number 10 October, *2015*

Medical Home NEWS

Can't I Just "Uber" My Doctor? Top 5 Legal Issues for Consumer-Facing Healthcare Technology

By Jill H. Gordon, JD, MHA and Daniel R. Eliav, JD, MPH

As the innovation of new healthcare technologies continues to expand, consumer interfacing platforms that connect consumers with providers in the market – think Uber, Expedia, or Amazon for healthcare – are invading and disrupting the way we think about access and delivery of care in the traditional healthcare space.

Inevitably, these technologies will become an integral part of every patient-centered medical home. Regardless whether the software is loaded on a computer, smart phone, wearable device, or some other piece of hardware, these tools have great potential to strengthen the patient-physician connection and improve health outcomes. With time, a few of these platforms will become the preferred option for some forms of care delivery and access. However, until that time, providers will be faced with the task of sifting through a myriad available software applications and vendors, and will be challenged with choosing the right one for their practice. As with almost any activity in health care, there are legal implications to be considered when making that choice.

Some of the more critical threshold legal issues are:

1. Whether the platform itself and its purported business model are legal
2. Whether there are potential fraud and abuse concerns triggered by participating in the platform
3. Whether the reimbursement model for services will change due to the platform (e.g., patients paying cash or utilizing coupons)
4. Whether the platform is private and secure
5. Whether the platform is compliant across state lines (if necessary)

If the platform holds itself out to the public as providing care, it will need to meet the same legal requirements as any other provider for the healthcare services. However, if it is simply a technology platform utilized by the provider, typically no additional licensure will be required.

The first question grapples with the many federal and state laws that govern what providers are and are not allowed to do, and also focuses on what the technology platform itself purports to do. Does the platform purport to be a delivery mechanism for care, or does it merely act as a means to locate and identify a provider, allow a consumer to check pricing, or prepay for certain services? Typically there are far more regulatory issues to address if care is provided through the platform; however, even if it is more of a referral service, it may still be subject to legal constraints. For those platforms through which providers render care, licensure is usually the first consideration among these rules. If care is provided through the platform, is the care provided by the underlying provider with a license to access the vendor's software, or is the vendor/platform providing care itself?

If the platform holds itself out to the public as providing care, it will need to meet the same legal requirements as any other provider for the healthcare services. However, if it is simply a technology platform utilized by the provider, typically no additional licensure will be required. If the platform itself is not a provider, would it be deemed a payor or be required to be licensed as a health plan under state law? If it's not a payor or provider, what is it? Is it a marketer? The answers to these questions will drive the regulatory structure and provide the over-arching basis for how to identify whether the platform is legally operating.

(continued on page 2)

Can't I Just "Uber" My Doctor? *…continued from page 1*

Does it Create Fraud and Abuse Concerns?

In addition to licensure issues, there are a wide variety of fraud and abuse laws that may impact the arrangement between the company providing the IT platform and the practitioner, and ultimately, patients. Some have tried to limit potential liability by specifically excluding government program business from these arrangements. However, state law may also present risk, and therefore, merely limiting services to the "cash pay" patients is not a sure path to compliance. Some of the "hot spots" to look out for with respect to potential fraud and abuse concerns include, "per-click" or other variable pricing for the IT platform, offers of discounts or fee waivers to patients for clinical services, referral or marketing services, and treating patients with high deductible health plan coverage as if they are "cash pay."

Will You Get Paid?

Once you have determined that an activity is allowed, the next consideration is whether it is reimbursable. For government payment programs, reimbursement will be determined by the applicable federal or state regulations. For commercial payors, reimbursement is a contractual matter. For instance, currently, Medicare only covers telemedicine in very limited circumstances. An interesting issue for the patient-centered medical home, and one that will likely see a lot of attention in the near future, is how to use consumer interfacing applications to qualify for reimbursement under Medicare's recently adopted Chronic Care Management CPT codes. Apps that can record the time a practitioner spends providing non-face-to-face care may prove to be extremely useful for providers who are trying to meet the minimum time required to bill these new codes every month. Increasingly, private insurers are appreciating the benefits of these types of applications as well and, in some instance, apps can be used to bolster accreditation and other metrics which may help improve reimbursement dollars.

An interesting issue for the patient-centered medical home, and one that will likely see a lot of attention in the near future, is how to use consumer interfacing applications to qualify for reimbursement under Medicare's recently adopted Chronic Care Management CPT codes.

Is it Private and Secure?

Further, a critical question is whether the software is private and secure. An analysis of privacy issues will usually be governed by the Health Insurance Portability and Accountability Act (HIPAA) as well as applicable state laws. Some application developers seem to be astutely aware of the privacy concerns and acknowledge their status as "Business Associates" through well drafted notices posted on their websites or integrated within their app. On the other hand, some developers seem to be totally oblivious to these concerns, and some go as far as erroneously stating on their webpages that HIPAA does not apply to their services. Regardless whether the parties have a business associate agreement in place or believe to be exempt from HIPAA, the privacy and security rules require compliance, and there are stiff penalties in the event of a data breach. For these reasons, it is important to have counsel well versed in privacy law to help navigate these issues.

An integral part of ensuring patients' privacy is that the software must also be secure. With constant attacks to information systems from overseas and within the United States, the hackability of any app -- as well as the location of the storage of the information – should be an important consideration.

Is it Compliant across State Lines?

The variability of applicable rules across state lines challenges software developers to create platforms and business models that are compliant with federal law as well as the laws of the 50 states. Licensure, privacy and security laws, fraud and abuse considerations, and advertising rules are just some of the considerations that are governed by specific state laws, which will be unique to operating in the state. Further, as remote monitoring and telehealth gain broader acceptance, it is the law of the patient's location, not the provider's location, that governs. This consideration can create challenges to doing business in multiple jurisdictions.

… as remote monitoring and telehealth gain broader acceptance, it is the law of the patient's location, not the provider's location, that governs. This consideration can create challenges to doing business in multiple jurisdictions.

Bottom Line

While the above analysis is only an introduction to the variety and complexity of legal issues, we hope that the above framework will provide assistance and a reference point as you contemplate integrating consumer interfacing software with your practice.

Jill Gordon is a Partner in the firm of Nixon Peabody, based in the Los Angeles office. She can be reached at jgordon@nixonpeabody.com.
Daniel Eliav is an Associate in the firm's Los Angeles office. He may be reached at deliav@nixonpeabody.com