THE TEXAS LAWBOOK

SERVING BUSINESS LAWYERS IN TEXAS

Digital Health and Telemedicine

By Todd Kelly and Courtney Carrell of Jones Day – (Nov. 8, 2017) – The Centers for Medicare & Medicaid Services estimates U.S. health care spending will total $5.5 trillion by 2025, which would then account for nearly 20 percent of the country's gross domestic product.

Todd Kelly

The digital health market is expected to exceed $200 billion by 2020, with one estimate predicting that the digital health industry will surpass $379 billion by 2024. Many digital health companies and startups looking for a share of this market are headquartered right here in Texas.

Broadly defined, digital health refers to several categories of technology-driven health care products and services, including the following:

- Health information technology (HIT), which refers to information technology applied to health care, including e-prescribing platforms and electronic medical records.
- Mobile health (mHealth), which refers to the use of smartphones and tablets to deliver health care, such as secure texting or diagnostic apps. Some mHealth apps work with wearable devices, such as contact lenses that monitor glaucoma or a necklace that detects cardiac arrhythmias.
- Software as a medical device (SaMD), which is software intended for medical purposes that is available on general purpose devices, like smartphones. It includes software designed for diagnostic or treatment purposes, such as computer software that allows a physician to view MRI images electronically. It does not include software that is part of another medical device, like an infusion pump.
- Telemedicine or telehealth, which generally refer to the use of technology to facilitate a physician's visit with a remotely-located patient. Telemedicine may be "synchronous," using a real-time video interaction between the patient and physician, or "asynchronous," with texts and photos sent back and forth (also known as "store-and-forward"). Services are sometimes provided through a physician intermediary, such as when a patient goes to a family doctor's office and receives a telemedicine consultation from a remote specialist. Or telemedicine may be provided directly to patients, such as when a patient uses an app or computer from home to access a doctor.

Recent legal developments propelling growth in digital health

Courtney Carrell

In addition to evolutions in technology, recent developments in state and federal law have facilitated widespread investment in Texas and beyond in the burgeoning digital health industry.

Until May 2017, Texas had some of the most onerous restrictions in the country affecting a key segment of digital health—telemedicine. The state severely limited direct-to-consumer telehealth options by requiring that most patients have a prior in-person visit with the physician before having a telemedicine visit with that doctor. The Texas Medical Board threatened disciplinary action against physicians who did not comply and was embroiled in antitrust litigation trying to defend its regulations.

While previous legislative efforts failed, this year stakeholders and lawmakers came together to support and unanimously pass Senate Bill ›

1107, which eased restrictions on telemedicine and resolved the multiyear litigation. Under the new law, a practitioner-patient relationship may be created through telemedicine using nearly any form of technology, so long as the provider meets the standard of care applicable to in-person visits.

The Texas law distinguishes between "telemedicine" and "telehealth," whereas many states do not. Telemedicine is defined as a health care service delivered through technology by a physician or other provider under the delegation of a physician (such as a nurse practitioner) when the provider is in a different physical location from the patient. The term telehealth is used when the health care service is delivered by a licensed health professional who may not be a physician or acting under a physician's supervision (such as a psychologist or physical therapist). These definitions open the door for both physicians and non-physicians to provide remote services directly to patients instead of requiring the use of in-person physician intermediaries.

On the federal side, the Food and Drug Administration is updating its oversight of SaMD and other digital health technologies. It recently launched the Digital Health Software Precertification Pilot Program to identify companies that demonstrate a culture of quality and excellence to enable such companies to have software programs fast-tracked for approval.

The FDA also announced plans to publish interpretive guidance on the 21st Century Cures Act (the 2016 law designed to help accelerate medical product innovation while reducing regulatory burden), including guidance on clinical decision support software.

Potential legal issues regarding digital health

While these legal developments have paved the way for digital health advancement, significant legal and regulatory challenges remain for providers, payers and manufacturers.

State licensure and liability

As the Texas example makes clear, state medical boards have varying incentives to regulate and sometimes restrict digital health initiatives. With each state governing the practice of medicine within its own borders, national telemedicine companies must navigate a labyrinth of state-specific laws and regulations to comply with professional conduct and licensure standards.

For example, some states restrict telemedicine providers from issuing prescriptions while others prohibit asynchronous services. Some states permit out-of-state licensed physicians to provide telemedicine while others require in-state licenses.

The Interstate Medical Licensure Compact created an expedited licensing process to enable physicians to practice in multiple states, but only 22 states participate, and implementation has been delayed in some locales due in part to difficulties obtaining federal background checks.

Professional liability also differs across state lines. To date, there is very little data on telemedicine malpractice claims. Most direct-to-consumer telemedicine physicians are family doctors who generally have fewer malpractice claims than other specialists. Nonetheless, as telemedicine services increase, so will malpractice claims. Plaintiffs' lawyers may argue that a telemedicine service was inadequate and the physician should have recommended in-person treatment.

In Texas, by statute, telemedicine physicians must provide the patient with guidance on follow-up care and forward relevant medical records to the patient's primary care physician. These requirements may reduce the malpractice risk for telemedicine providers by shifting the burden of care to the patient's primary doctor. ›

Payment and reimbursement

As with state-specific regulations on the practice of medicine, each state also has its own insurance code and reimbursement regulations that may affect telemedicine contract negotiations with insurers.

Texas has "coverage parity," meaning that a private health plan may not exclude a telemedicine service from coverage solely because the service is not provided through an in-person consultation. Texas does not have "payment parity," however, so there is no requirement for health plans to reimburse telemedicine services at the same rate as in-person visits. This issue will likely be debated in the 2019 Texas legislative session.

Ultimately, the value of digital health may not be fully realized until health care moves closer to a value-based payment model. For example, a diabetes patient who frequently texts her doctor may have greater physician costs in a fee-for-service context, but the routine physician-patient interaction may eventually result in a better managed disease with fewer hospitalizations, reducing overall costs.

In the meantime, while the health care system continues to straddle value-based and fee-for-service compensation, telemedicine providers must navigate a patchwork of reimbursement models.

Privacy and cybersecurity

Nearly all health care providers—including digital health providers—that electronically transmit health information are "covered entities" and must comply with the privacy regulations in the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act.

HIPAA requires covered entities to maintain privacy safeguards to protect patient information, but most cybersecurity experts believe HIPAA is outdated. Although HITECH made some revisions to the law, the HIPAA-required safeguards have not been updated since 2003, despite a massive evolution in digital health technology. As health care providers introduce more internet-connected services and devices, covered entities need to think beyond HIPAA to protect their patients and data.

Cyberattacks threaten a provider's business operations, reputation and ability to treat patients, not to mention the company's bottom line. Last year, the health care industry was the victim in 88 percent of all ransomware attacks. The volume of these attacks reflects the value of health care data.

Forbes recently reported that a credit card number costs 25 cents on the black market, but an electronic medical record could be worth hundreds of dollars because it includes patients' employers, relatives' names, and medical diagnoses, among other sensitive information. This information may be used to blackmail or impersonate victims. A patient can change his credit card number but not his medical history.

Data ownership

The value of health data also affects the business strategies and intellectual property negotiations of providers and technology companies. Knowing exactly which symptoms, radiology image patterns and lab results indicate disease could lead to earlier diagnoses and access to life-saving treatment. This is valuable information that insurance companies, pharmaceutical companies, providers and patients may be willing to pay for.

But who owns this data? Does it belong to the electronic medical record company, the insurance company, the lab, the hospital or the patient? HIPAA only provides patients access rights, not ownership. In some states, by law, the provider owns the medical records, but these laws do not specifically address the data within the records or situations when there are multiple providers, such as a lab and a physician. ›

Likewise, the legal framework does not address devices that track data and send it directly to a provider. Does the cardiac data on the arrhythmia-tracking necklace belong to the provider, or could the device manufacturer use data mining to detect patterns and sell the results?

While the law leaves these questions unanswered, providers must recognize the value of their patient data and carefully consider ownership rights and data use terms when contracting with vendors.

Conclusion

Many hope that the rise of digital health will achieve what has proven elusive for traditional health care—providing necessary health services to Americans in a manner that improves outcomes while reducing costs.

Whether or not digital health can achieve this goal, we can be certain that these new technologies will transform health care delivery and the associated regulatory framework will need a transformation of its own.

The views and opinions set forth herein are the personal views or opinions of the authors; they do not necessarily reflect views or opinions of the law firm with which they are associated.

Authors:

Todd P. Kelly, partner in Jones Day's Health Care and Life Sciences Practice.

Courtney A. Carrell, associate in Jones Day's Health Care and Life Sciences Practice.

Lindsay Hedrick, Jay Johnson, and Samir Kaushik provided valuable comments for this article.