Hogan Lovells

Health care trends in a post-pandemic economy

The COVID-19 pandemic has led to the rapid expansion and widespread adoption of telehealth/telemedicine services, significantly altering how health care providers deliver—and how consumers access—medical services around the world.

While providers laid much of the groundwork for telehealth innovation prior to the pandemic, the health crisis served as a catalyst for implementing these alternative care models on an expedited basis. Given that many of these pandemic-inspired adaptations to health care services are likely to remain in a post-COVID world, health care providers should be aware of how these changes will affect their business in order to successfully navigate this new landscape.

Privacy and cybersecurity

The rapid adoption of new technologies to facilitate telehealth services during the pandemic has resulted in increased data and data flows, leading health systems and hospitals to grapple with novel questions pertaining to data arrangements and cybersecurity. It is important for health systems to understand the rules of the road with respect to data collaborations and transfers of patient information among health care providers. Given the necessary expediency required to roll out telehealth services during the pandemic, many of the rules in the U.S. permitting data collaboration and transfers were implemented through the use of temporary waivers or guidance given in the context of the public health emergency. In practice, this means that the pathways for these data flows and collaborations may have been carried out without the usual processes that govern such activities, and the same pathways may not persist post-pandemic.

The question for health care and technology companies seeking to build upon the expansion of their telehealth capabilities during the pandemic is what will be the new normal regarding regulation of these digital health initiatives? The collaboration of health care services and technology brings with it a number of concerns with respect to privacy and cybersecurity, including questions surrounding the types of permissions, notices and consents that are required to access telemedicine services, overall structure of the data arrangement, and the potential liability for data breaches or cyberattacks.

With the increased threat of ransomware attacks plaguing a variety of platforms, telehealth services will need to engage their entire organizations to work to protect their systems from bad actors looking to exploit technological vulnerabilities. In addition, breaches and cyberattacks may lead to costly litigation when data has been potentially exposed or lost.

Transactions and partnerships

At the start of the pandemic, hospital mergers and acquisitions slowed as providers focused on the crisis at hand and struggled with supply chain issues and decreased cash flow resulting from the suspension of elective surgeries. However, following receipt of government stimulus funds and

the resumption of elective surgeries, there was an acceleration of health care deals that has continued, specifically acquisitions of smaller health systems, hospitals and independent physician groups by larger health systems with stronger financial positions. The stress of the pandemic made it clear to many smaller providers that they needed to partner with a larger system, and given that around 30% of hospitals are still stand-alone the trend of smaller organizations joining larger health systems is likely to continue.

Another trend is the desire of health systems for better revenue diversification. There has been a recent increase in cross-sector deals, such as hospital systems seeking to acquire health plans. In addition, health systems are seeking to provide offerings all along the continuum of care, particularly in the outpatient setting. Following the pandemic, diversification is seen as providing much-needed balance for health systems. For example, by acquiring a health plan to serve as a natural balance to its inpatient care business, a hospital system can protect itself should an external crisis arise that would negatively affect a particular revenue stream (e.g. the suspension of hospital elective surgeries during the height of the COVID-19 crisis). Expect to see an increase in provider/payer deals, as well as transactions of hospital systems expanding into the outpatient space. It should be noted that the continued consolidation of the health systems in the U.S. will inevitably lead to scrutiny from federal antitrust regulators, as well as potential litigation from private antitrust plaintiffs.

International telehealth regulatory considerations

As telehealth gains prevalence around the globe, providers are increasingly looking to expand their telehealth programs to offer virtual care to patients internationally. While telehealth has many advantages, it also raises—in the international context—difficult questions of foreign regulation, the answers to which constitute a blurry patchwork from country to country. Some countries have not yet implemented a regulatory framework that governs telemedicine, and typically, the rules that govern traditional face-to-face medical care will apply. Other countries do have telehealth laws on the books, but often these laws only address circumstances where the physician and patient are both located within the same country. These issues lead to one of the most challenging aspects of international telemedicine: the question of whether and how physician licensing rules apply when the doctor and patient are located in different countries.

While the approach varies from country to country—and sometimes, from province to province within a country—peer-to-peer consultations generally tend to be less regulated than virtual interactions between a practitioner and a patient, since consultations between physicians with no direct patient interaction by the non-local practitioner are less likely to be considered the "practice of medicine" as defined by local regulations. In countries where peer-to-peer consultations are not governed by more stringent telehealth regulations, doctors who are already licensed in their home jurisdiction typically would not have to obtain additional licensure or registration in the foreign country to consult with other physicians in that country. Direct-to-patient telemedicine services, on the other hand, often require local licensure by the physician or local registration by the hospital providing the services, or both, and these processes can be burdensome and impractical.

As telehealth services make it easier for health care providers to provide cross-border care, it is increasingly necessary for providers to have a firm understanding of the local telehealth laws and regulations in each jurisdiction in which they seek to do business.

Preventing fraud and abuse in an expanding telehealth sector

The regulatory flexibility provided by the government during the pandemic allowed for a massive expansion of telehealth services covered by Medicare. Medicare's telehealth benefit only covers a very narrow set of office and hospital visits, with all telehealth services required to use audio-visual technology for a beneficiary located in a rural or health professional shortage area. Beginning in March 2020, CMS waived statutory restrictions and significantly expand telehealth services to all Medicare beneficiaries. As a result, in the United States there were approximately 350 times the number of telehealth visits in 2020 than

in previous years. This represents a sea change in the industry, and brings with it significant potential for fraud and abuse.

Most enforcement activity to date has reflected traditional fact patterns, such as claims for unnecessary prescriptions or services not rendered, which just happen to have been facilitated through telecommunications media. However, in May DOJ announced an indictment related to abuse of COVID-19 waivers, alleging that defendants "exploited temporary waivers of telehealth restrictions enacted during the pandemic by offering telehealth providers access to Medicare beneficiaries for whom they could bill consultations. In exchange, these providers agreed to refer beneficiaries to [defendants'] laboratories for expensive and medically unnecessary cancer and cardiovascular genetic testing."

Separate from pandemic-related matters, recent enforcement efforts have alleged that billions of false and fraudulent claims have been facilitated through telehealth submissions. The Department of Justice (DOJ) has charged a large number of individuals with fraud involving a number of different market participants, including durable medical equipment suppliers who use remote consultations to obtain personal information which is then used for fraudulent claims. Such schemes have been a focus of Centers for Medicare & Medicaid Services (CMS) and DOJ auditors, and legitimate providers should focus on conducting internal audits to identify any potential outliers where there are far higher claim rates with respect to the frequency or location of services.

Health care sector trends and developments in Germany and the EU

Recently, there has been increased interest by investors from the U.S. and China in German health care investment opportunities. Historically, the stationary and ambulatory sectors of Germany's health care industry have operated separately. However, more recently, these two sectors have been moving closer together, with telemedicine and AI increasing significantly in both areas.

Until 2016, Germany maintained very strict regulations prohibiting telemedicine. Since 2016, telemedicine has been permitted on a professional level. During the pandemic, investment and interest accelerated with respect to remote treatment in the ambulant sector as well as peer-to-peer telehealth consultations. There is also a lot of interest in other markets in Europe from international investors.

Closely related to the telemedicine sector are regulatory considerations governing data protection and data use. When the European Union General Data Protection Regulation (GDPR) became law on 25 May 2018, awareness with respect to the importance of protecting sensitive personal health data by health care providers and other involved third parties has been increasing steadily. There have also been discussions about how restrictively to interpret the law protecting personal data while balancing considerations of how that data can be used on an anonymized basis within the pharmaceutical and health care sectors to benefit all stakeholders, in particular patients. This is a significant area of debate that will likely be a focus on both a national level in Germany and across the EU.

Conclusion

The health care industry has faced incredible challenges throughout the pandemic which has led to significant and lasting changes to how medical services are provided and accessed around the world. Providers should be aware of what these changes mean for their business, and consult experienced counsel for guidance in navigating this evolving health care landscape.