BLANKROME

Healthcare

MAY 6, 2020 • NO. 2

As Federal and State Governments Push for Expanded Telehealth Services, Healthcare Providers Must Proceed Carefully to Avoid and Mitigate Risk

Our last client alert described important considerations for healthcare providers expanding their telemedicine services in response to the coronavirus COVID-19 outbreak as the legal landscape rapidly changes. In this follow-up alert we highlight additional ways the federal government is promoting telehealth expansion, including through funding, business support, and policy guidance. We also address the significant potential pitfalls facing providers as they integrate telemedicine services into their business. Companies transitioning to or expanding their telehealth capabilities must proceed carefully with an understanding of applicable policies and licensing requirements.

The Federal Government Is Actively Encouraging Telehealth Services

To date, under the CARES Act the Department of Health and Human Services ("HHS") has awarded $150 million to 1,779 health centers and $11.5 million to 14 Health Resources and Services Administration ("HRSA")-funded Telehealth Resource Centers to assist rural and underserved communities combat COVID-19. The Federal Communications Commission ("FCC") has also instituted a COVID-19 Telehealth Program through the CARES Act to provide up to $200 million for the purchase of telecommunications, information services, and connected devices by nonprofit and public healthcare providers[1], including both rural and non-rural health clinics, to support the implementation and development of "Connected Care" services, which includes telehealth services.[2] Thus far under this program, the FCC has awarded approximately $13.7 million in grants to 30 telehealth projects in 16 states.

HHS has launched a website to provide healthcare providers with information they need to better integrate telehealth services into their business, understand applicable policies (including those that have been adopted in connection with the COVID-19 outbreak), and make certain they have what patients will need to be able to use telehealth. The website includes region- and practice-specific telehealth guides for healthcare providers and resources to assist providers in selecting appropriate technology vendors and set up workflows to schedule and manage telehealth appointments. It also summarizes important legal considerations for telehealth providers, including as they relate to cybersecurity, privacy, informed patient consent, malpractice liability, and state licensing requirements. (As of April 29, 2020, the District of Columbia and all states except Arkansas had adopted licensure requirements in response to the COVID-19 outbreak (if they had not already done so) to permit physicians licensed in other jurisdictions to provide telemedicine services to patients in state.)

The Centers for Medicare & Medicaid Services ("CMS") recently published a COVID-19 Telehealth Toolkit, designed to guide states' coverage of telehealth services by state Medicaid and Children's Health Insurance Programs. The Toolkit provides a comprehensive checklist that identifies specific policy considerations for states, including, for example: (1) applicable privacy laws for pediatric patients; (2) how existing payment methodologies might restrict or prevent service delivery through telehealth; and (3) provider licensure and credentialing in Medicaid, and whether a provider's professional scope of services enables him or her to bill for a telehealth service. CMS has announced that it will provide updates to the Toolkit to highlight specific telehealth policies implemented by states throughout the COVID-19 emergency.

Cybersecurity Is a Significant Concern

Cybersecurity threats pose a major concern for the delivery of telemedicine services. Home computer systems and personal devices used by healthcare providers are vulnerable to viruses, phishing, malware, and hacks. Additionally, most connected medical devices, such as pacemakers, insulin pumps, or stimulators, do not have security parameters which leaves them vulnerable to security breaches as well. For example, in March 2020 the Food and Drug Administration issued a press release warning patients, providers, and manufacturers about potential cybersecurity vulnerabilities in certain medical devices with Bluetooth Low Energy, which can allow a hacker to interfere with the device.

Criminals have preyed on these vulnerabilities to disrupt healthcare providers' businesses. As a result, an increasing number of providers are experiencing ransomware and other cyberattacks aimed at stealing or corrupting patient data.

Government Scrutiny of Telehealth Providers Is Increasing

The U.S. Department of Justice has announced repeatedly and emphatically its intent to prosecute individuals and entities seeking to capitalize on the pandemic to engage in fraud. This stated enforcement priority naturally encompasses healthcare providers, including those involved in telemedicine services. On March 30, 2020, the United States Attorney for the District of New Jersey charged an individual with conspiracy to violate the Federal Anti-Kickback Statute and to commit healthcare fraud for allegedly soliciting and receiving kickbacks in connection with unnecessary clinical testing. The criminal complaint alleged that the charged individual located Medicare beneficiaries who were not exhibiting symptoms of COVID-19, and then arranged for telemedicine healthcare providers to send these pre-screened beneficiaries prescriptions for COVID-19 tests bundled with a more expensive respiratory pathogen panel ("RPP") test, which does not identify or treat COVID-19. In exchange for kickbacks, the charged individual would then refer these beneficiaries to laboratories to conduct the prescribed clinical testing.

Additionally, on April 23, 2020, the United States Attorney for the Southern District of Georgia charged a telemedicine company owner in connection with an alleged $60 million fraud scheme involving fraudulent orders for durable medical equipment ("DME"). The case arose out of coordinated government efforts in 2019, dubbed "Operation Brace Yourself" and "Operation Double Helix," to root out fraud in connection with DME and genetic testing. These efforts reflect the U.S. Department of Justice's increasing scrutiny of telemedicine services and led to the prosecutions of several telemedicine providers in multiple jurisdictions over the last year.

Healthcare Providers Must Proceed Carefully as They Expand Their Telemedicine Services

Telemedicine offers tremendous opportunity to healthcare providers seeking to continue servicing patients in this age of stay-at-home and shelter-in-place orders. Providers must nonetheless remain cognizant of the potential pitfalls that come with the industry-wide expansion now being fueled by government support. They should review their malpractice and liability policies to ensure that they apply to the specific telemedicine services offered. To address pervasive cybersecurity and privacy concerns, providers should consider implementing best practices, such as: utilizing VPN, multifactor authentication, or other methods of identity authentication to protect information; entering into business associate agreements with technology vendors; and avoiding communicating protected health information in public spaces. Providers must also be diligent in maintaining necessary patient records, including signed informed consent forms. Notably, the specific requirements for informed consent forms varies by state. Providers should carefully review them to ensure compliance in the state or states in which they do business.

Considering the rapidly changing legal landscape, providers should have in place effective compliance programs and billing procedures to ensure compliance with applicable

state and federal policies. Moreover, government agencies, including the U.S. Department of Justice and other state and federal law enforcement authorities, will vigorously pursue companies and individuals that unlawfully take advantage of the system by trying dishonestly to reap government funds or by avoiding compliance with applicable policies or licensing requirements. As such, healthcare providers must be truthful in any disclosures they make to the government.

Blank Rome's Coronavirus ("COVID-19") Task Force is continuing to monitor the COVID-19 crisis and will provide further updates as they become available.

For additional information, please contact:

Ariel S. Glasner, Washington, D.C. Office
Partner, White Collar Defense and Investigations
202.772.5963 | aglasner@blankrome.com

Jane Thomas, Washington, D.C. Office
Associate, General Litigation
202.420.2577 | jthomas@blankrome.com

1. These include: (1) post-secondary educational institutions offering healthcare instruction, teaching hospitals, and medical schools; (2) community health centers or health centers providing healthcare to migrants; (3) local health departments or agencies; (4) community mental health centers; (5) not-for-profit hospitals; (6) rural health clinics; (7) skilled nursing facilities; or (8) consortia of healthcare providers consisting of one or more entities falling into the first seven categories.

2. "Connected Care services is broadly defined as a subset of telehealth that uses broadband Internet access service-enabled technologies to deliver remote medical, diagnostic, patient-centered, and treatment-related services directly to patients outside of traditional brick and mortar medical facilities—including specifically to patients at their mobile location or residence. Examples of connected care services delivered to patients at their residence or mobile location rather than a health care provider's physical location include, but are not limited to, remote patient monitoring (e.g., use of patient reporting outcome platforms, glucometers, pulse oximeters, sphygmomanometers, chest straps, wearables, passive sensors, or other devices to consistently monitor patient vitals), patient health education, store and forward services (e.g., asynchronous transfer of patient images and data for interpretation by a physician), and synchronous video consultations and visits." FCC Order, at p. 10, docs.fcc.gov/public/attachments/FCC-20-44A1.pdf.