COSMOS
Navigate the Compliance Universe

Compliance Today - February 2024

Harini Pallavi (harini.pallavi@friggp2c.com, linkedin.com/in/harini-mandavilli-7bb5a032/)
is Chief Operating Officer at Frigg Business Solutions Inc. in Sheridan, WY.

Sidestep these telehealth compliance minefields

by Harini Pallavi Mandavilli

Formerly known as telemedicine, telehealth came to be recognized as a valid, viable treatment option by insurance carriers—especially Medicare and Medicaid—in the 1990s. However, its increasing importance for providers and patients alike was realized in the new millennium, especially after the insistence on the switch from paper records to electronic health records (EHRs) in the American Recovery and Reinvestment Act of 2009. The recent coronavirus pandemic further underscored the benefits and significance of telehealth.

Benefits of telehealth

The greatest benefit of telehealth is that patients living in hard-to-reach areas, such as mountainous regions, can receive medical advice in an emergency. This means saving lives as well as protecting people from the crippling effects of delayed treatment of certain ailments. It means patients have greater access to high-quality specialist treatment, which they might have been denied otherwise. There are concomitant cost savings for patients and facilities, given the reduction in readmissions due to appropriate follow-up and monitoring of patients recently discharged from acute care or post-acute care facilities.

For the providers: It means not only enhanced revenues but also increased patient engagement and satisfaction. This, in turn, implies that there is greater patient loyalty. With patient protected health information (PHI) being available as EHRs, the numerous patient portals have made access to patients by doctors and vice versa so much easier. The biggest advantage of telehealth is that it assures a continuum of care. However, as with all good things, there are downsides.

Watch out for impermissible telehealth models

There are numerous compliance landmines that you would do well to negotiate with care. Healthcare providers—facilities, doctors, clinics, or path labs—need to be wary of getting into telehealth models, which could potentially put them in the U.S. Department of Health and Human Services (HHS) Office of Inspector General's (OIG) crosshairs. OIG focuses on fighting fraud, waste, and abuse of the welfare measures of the federal government. Therefore, any healthcare provider that adopts a telehealth model, which fails to delimit virtual encounters, risks being investigated or prosecuted for participating in or entering a financial arrangement that violates the Stark Law and Anti-Kickback Statute (AKS).

Financial arrangements prohibited under Stark Law and AKS

If Medicare and Medicaid are billed for services, then the Stark Law categorically prohibits a wide range of financial relationships between doctors and healthcare facilities with other healthcare providers like path labs,

radiology units, dialysis centers, skilled therapists, manufacturers of durable medical equipment, pharmacies, or even pharmaceutical companies. In a prosecution under Stark Law, there is no need for proof of intention to induce a referral subsequently. However, in an AKS prosecution, the intent to induce referrals must be established even if the action has begun based on a whistleblower's complaint. As a covered entity (CE), you need to verify state laws governing income sharing and other financial arrangements with third parties.

So, how does all this impact telehealth services?

Different states have their individual laws regarding licensure for professionals. Under such circumstances, you must verify whether the state where the patient resides allows medical professionals from another state to treat them, even if it is virtually. Virtual monitoring will be effective only when doctors and caregivers cooperate and there are appropriate protocols to provide additional support. You must also maintain medical records scrupulously in accordance with the licensure requirements of your specialty. Remember, if one or more patients are suspected of receiving improper care through telehealth, pharmacies and others may decline to fill prescriptions or provide services for that doctor's patient.

DOJ cracks down on fraudulent telemedicine claims

In a press release in July 2022, the U.S. Department of Justice (DOJ) referred to federal investigations into schemes "involving the payment of illegal kickbacks and bribes by laboratory owners and operators in exchange for the referral of patients by medical professionals working with fraudulent telemedicine and digital medical technology companies. Telemedicine schemes account for more than $1 billion of the total alleged intended losses . . ."[1] Unfortunately, in most cases, neither was the genetic testing for cardiovascular disease and cancer needed, nor was the equipment delivered to the beneficiary. In some cases, the reports of tests were not used in drawing up the treatment plan.

Deviously crafted kickback schemes: In the same press release, Inspector General Christi A. Grimm referred to the partnership of OIG and law enforcement authorities to uncover "fraud schemes that use the guise of telehealth to expand the reach of kickback schemes designed to cheat federally funded health care programs."

Virtual sign-ins: Telehealth uses various kinds of electronic information and telecommunication technologies such as video teleconferencing and messaging apps or simply using landlines or mobile phones for the doctor and patient to speak to each other. Sometimes, certain technologies must be used with caution. For example, virtual sign-ins for doctor appointments are permissible only if the patient is an existing one. New patients cannot utilize that provision before a physical encounter.

Healthcare providers cannot evade responsibility for being compliant

Anywhere there is recording, storage, and/or exchange of PHI, the fear of data breach and the overarching need for assuring data security exists. This indicates that doctors must ensure a secure connection while providing telehealth services. Most telehealth services need the support of third-party vendors such as telecommunication service providers for real-time interactions, web-based services such as monitoring services, and cloud platforms that facilitate storage of PHI and encounter notes to carry forward where needed. This means that neither the doctors nor the providers who support telehealth can evade their responsibility to be compliant with the provisos of HIPAA, its allied rules—Privacy, Security, Breach Notification, and Omnibus[2] —and the requirements of frameworks such as Health Information Trust Alliance and National Institute of Standards and Technology.

Settings in which telehealth services may be furnished

Providers might need to educate their patients—in the case of pediatricians, the parents of their patients—about the need for secluded settings for virtual encounters, which are furnished via real-time, interactive communication technology. Patients must be told that the entire purpose of providing healthcare virtually is to enable those who live far from even primary healthcare facilities. During the pandemic, the need to reduce the spread of infection in the community was also a major concern. Therefore, virtual encounters should not occur when either the patient or the doctor needs to be in a public or semipublic place, especially when PHI needs to be shared.

Privacy requirements you must not overlook

Given that telehealth refers to healthcare services provided through "the use of electronic information and telecommunications technologies to support and promote long-distance clinical healthcare, patient and professional health-related education,"[3] it becomes critical that providers keep a close eye on the HIPAA privacy requirements which every CE must comply with. HHS Office for Civil Rights (OCR) reminds healthcare providers to conduct all telehealth services in private settings to assure compliance with HIPAA and its allied rules.

OCR states on the HHS website, "If telehealth cannot be provided in a private setting, covered health care providers should continue to implement reasonable HIPAA safeguards to limit incidental uses or disclosures of protected health information."[4]

Expansion of telehealth services during the pandemic

The recent pandemic demonstrated the value of telehealth services in not only assuring healthcare to those who were housebound due to the lockdown but needed urgent or follow-up care. It also proved valuable in reducing and even preventing the community spread of the coronavirus. The 1135 waiver during the pandemic meant that "Medicare can pay for office, hospital, and other visits furnished via telehealth across the country and including in patient's places of residence starting March 6, 2020," according to the Medicare telemedicine healthcare provider fact sheet.[5] It further stated, "Starting March 6, 2020, and for the duration of the COVID-19 Public Health Emergency [PHE], Medicare will make payment for professional services furnished to beneficiaries in all areas of the country in all settings."

Conclusion

Prior to the onset of the pandemic, there were numerous limitations on telehealth practice, including access to technology, the kind of reimbursement being offered, and the cross-border licensure requirements. Now that the PHE has ended, staying abreast of the latest legal developments regarding telemedicine and e-health services is in your best interest.

Takeaways

- While the benefits of telehealth are numerous and have been well demonstrated during the recent public health emergency, it poses many compliance challenges.
- Certain telehealth models are impermissible under regulations like Stark Law, Anti-Kickback Statute, and the False Claims Act.
- Stay alert to cross-border licensure requirements.
- Never lose sight of the requirements of HIPAA Security and Privacy rules and security frameworks like the

Health Information Trust Alliance and the National Institute of Standards and Technology.

- Relaxations spurred by the coronavirus pandemic have ended. Stay alert to legal developments.

1 U.S. Department of Justice, Office of Public Affairs, "Justice Department Charges Dozens for $1.2 Billion in Health Care Fraud," news release, July 20, 2022, https://www.justice.gov/opa/pr/justice-department-charges-dozens-12-billion-health-care-fraud.
2 U.S. Department of Health and Human Services, "HIPAA for Professionals," content last reviewed May 17, 2021, https://www.hhs.gov/hipaa/for-professionals/index.html.
3 U.S. Department of Health and Human Services, "What is telehealth?" content last reviewed March 27, 2020, https://www.hhs.gov/hipaa/for-professionals/faq/3015/what-is-telehealth/index.html.
4 U.S. Department of Health and Human Services, "Where can health care providers conduct telehealth?" content last reviewed March 27, 2020, https://www.hhs.gov/hipaa/for-professionals/faq/3021/where-can-health-care-providers-conduct-telehealth/index.html.
5 Centers for Medicare & Medicaid Services, "Medicare Telemedicine Heal Care Provider Fact Sheet," March 17, 2020, https://www.cms.gov/newsroom/fact-sheets/medicare-telemedicine-health-care-provider-fact-sheet.