COSMOS
Navigate the Compliance Universe

Complete Healthcare Compliance Manual
Patient Care: Telehealth and Telemedicine

Raul G. Ordonez, CHC; Vice President & Chief Compliance Officer; Jackson Health System[1]

What are Telehealth and Telemedicine?

The terms "telehealth" and "telemedicine" are commonly used interchangeably, and their definitions may vary depending on the location or jurisdiction where defined. Generally, "telemedicine" refers to the delivery of healthcare whereby the healthcare provider can care for the patient from a remote location through the use of electronic telecommunication. The term "telehealth" commonly has a broader connotation that includes both provider-patient encounters as well as the use of electronic telecommunication for other health-related interactions including provider education, public health, and health administration."[2] For purposes of this article, the terms will be used interchangeably, but with a narrower focus in the context of provider-patient care.

For years, advocates of telehealth have emphasized its ability to expand access to healthcare services not readily available, improve patient convenience and experience, and lower provider costs. Moreover, they have continually predicted that telehealth will feature prominently in the future delivery of healthcare. Meanwhile, consistent with those predictions, the use of telehealth has grown considerably in just a few years with more insurance plans covering telehealth services, more providers offering them, and more states regulating the services in their respective jurisdictions.[3] The predicted growth in telehealth was further intensified by the COVID-19 pandemic. Despite its increasing availability and practice prior to COVID-19, Medicare reimbursement was primarily limited to services for patients located in qualifying rural areas. However, in response to the COVID-19 pandemic, the Centers for Medicare & Medicaid Services (CMS) relaxed a number of the requirements that had been necessary for reimbursement and temporarily expanded the types of telehealth services for which Medicare reimbursement is available.[4] Almost three years after the onset of the public health emergency (PHE), though the permanence of Medicare reimbursement for specific services may still be unclear, there is a general consensus that the pandemic has accelerated the practice of telehealth in a manner that is to some degree irreversible. As stated by then CMS Administrator Seema Verma in 2020, the COVID-19 pandemic has taken telehealth to a new frontier, and, "there's absolutely no going back."[5] The same general sentiment is still present as of the time of this writing.

Correspondingly, the growth in telehealth over the years has resulted in increasing government scrutiny. Even prior to the pandemic in April 2018, when Medicare reimbursement was far more limited, the HHS Office of Inspector General (OIG) already had an interest in telehealth due to its relatively rapid expansion up to that point. At the time, the OIG published its audit findings identifying the failure by providers to meet various Medicare requirements.[6] Subsequently, as a result of the substantial expansion of services during the PHE, the OIG has signaled an even greater interest in telehealth by adding thirteen telehealth-related reviews to its annual work plan since the onset of the pandemic.[7] In addition, there have been a number of large-scale prosecutions by the Department of Justice (DOJ) alleging over $1 billion in fraudulent activity involving telemedicine companies and fraudulent relationships with physicians.[8] Correspondingly, the OIG published a Special Fraud Alert regarding fraudulent contractual arrangements between physicians and telemedicine companies .[9] All in all, there is considerable evidence that telehealth-related noncompliance is a growing government enforcement priority.

Given the continued growth of telehealth happening even before and especially during the COVID-19 public health emergency, it is reasonable to expect government enforcement efforts to further intensify.

Risk Area Governance

Medicare and Medicaid Program Integrity Provisions

Social Security Act § 1128J(d)[10]

This law requires that any self-identified Medicare overpayments resulting from incorrect coding, insufficient documentation, and medical necessity errors be returned within 60 days of identification.

Anti-Kickback Statute

42 U.S.C. § 1320a-7(b)[11]

The Statute prohibits offering, paying, soliciting, or receiving anything of value to induce or reward referrals to generate federal healthcare program business.

See article "Anti-Kickback Statute" in Chapter 5 for more information about the law.

The Stark Law

42 U.S.C. § 1395nn[12]

The Stark Law prohibits a physician from referring Medicare patients for designated health services to an entity with which the physician (or physician's immediate family member) has a financial relationship, unless an exception applies.

See article "Physician Self-Referral Law (Stark Law)" in Chapter 5 for more information about the law.

False Claims Act

31 U.S.C. §§ 3729–3733[13]

The False Claims Act prohibits, among other things, (1) the submission of false or fraudulent claims and (2) knowingly making, using, or causing to be made false statements or information to obtain fraudulent claims payment. False Claims Act violations occur when providers knowingly bill for services improperly. In addition, violations of both the Anti-Kickback Statute and the Stark Law as well as the failure to refund overpayments can each result in False Claims Act liability.

See article "False Claims Act" in Chapter 5 for more information about the law.

Health Insurance Portability and Accountability Act (HIPAA)

Pub.L. No. 104-191, 110 Stat. 1938[14]

HIPAA imposes requirements upon "covered entities" including healthcare providers, healthcare plans, and clearinghouses regarding their transmission of protected health information (PHI). PHI is information created or received by the covered entity that identifies an individual and relates to the individual's health or healthcare provision, or payment thereof. Under HIPAA, covered entities must handle PHI as required by the Privacy Rule[15]

, Security Rule[16] , and Breach Notification Rule[17] . Under the Privacy Rule, covered entities can only use and share PHI after obtaining patient authorization unless a specific HIPAA exception applies. The Security Rule requires covered entities to maintain administrative, physical, and technical safeguards to assure the confidentiality, integrity, and availability of the PHI. The Breach Notification Rule requires covered entities to notify the Secretary for Health and Human Services in the event of a breach of unsecured PHI.

See article "Health Insurance Portability and Accountability Act of 1996" in Chapter 5 for more information about the law.

Ryan Haight Act

21 U.S.C. § 829(e)[18]

This act amended the Controlled Substances Act to prohibit the delivering, distribution, or dispensing of a controlled substance by means of the Internet without a valid prescription.[19] This requires that the prescription be issued for a legitimate medical purpose either by a practitioner having conducted at least one in-person medical evaluation or by a covering practitioner. The regulations provide seven telemedicine exceptions to the in-person examination requirement.[20] They include:

- The practice of telemedicine while the patient is being treated by and physically located in a qualifying hospital or clinic.
- The practice of telemedicine while the patient is in the physical presence of a practitioner.
- The practice of telemedicine by a practitioner who is an employee or contractor of the Indian Health Service.
- The practice of telemedicine during a public health emergency as declared by the Secretary of HHS.
- The practice of telemedicine when conducted by a practitioner who has received a special registration from the DEA Administrator.
- The practice of telemedicine that occurs in a Department of Veterans Affairs medical emergency.
- The practice of telemedicine in circumstances specified by DEA regulation.[21]