The Doctor is in (and Online): A Look at Telehealth Fraud

Jennifer Trussell
Consultant

Telemedicine is the provision of health-related services through computers, video applications, smart phones, and other digital communication technology. Telehealth is a broader term that can include nonclinical services, such as continuing medical education, but the two terms are often used interchangeably. Telehealth is promoted as an advancement in medicine that will increase access to health care, improve health care gaps and chronic disease management, mitigate provider shortages, expand the availability of specialists, and potentially decrease the cost of health care. As with most health care services, both are also susceptible to fraud.

Telehealth Overview

Numerous articles, often sponsored by technology companies looking for a growth market, tout the skyrocketing rate of telehealth services. However, a recent study led by the Harvard T.H. Chan School of Public Health found that although there was an increase in these services over the last decade, its use is still uncommon. The study did highlight that there was a more notable increase in the use of telehealth by primary care physicians in more recent years, especially associated with younger patients in urban areas. The study also drew attention to the increase in telemental services (for behavioral health), especially in hospitals and rural areas where there are provider shortages.

While only broadly considered a telehealth service, the use of secure texts/emails and online patient portals for accessing reports and messages is becoming commonplace for outpatient services. Patient portals are also increasingly being used to distribute medical educational materials, such as articles and videos.

Main Types of Telehealth

There are three main types of telehealth services. The first is synchronous telehealth, which includes real-time video conversations such as office visits and consultations with specialists. The second is asynchronous telehealth, also known as

store-and-forward communication. Asynchronous services include the sharing of patient information between providers, such as imaging and laboratory reports. The third type is remote patient monitoring. Also known as telemonitoring, it uses technology, often in real time, to electronically monitor and transmit patient information such as vital signs.

While only broadly considered a telehealth service, the use of secure texts/emails and online patient portals for accessing reports and messages is becoming commonplace for outpatient services. Patient portals are also increasingly being used to distribute medical educational materials, such as articles and videos. Telehealth can be both inpatient and outpatient.

Hospital Telehealth

The rate of telehealth expansion in hospital settings appears to be growing more rapidly than traditional outpatient services. A telehealth fact sheet published by the American Hospital Association noted that in 2010 only 35% of hospitals were using a computerized telehealth system. In 2017, that number had risen to 76%. Hospital-based telehealth services include asynchronous services and remote patient monitoring. Hospital-based asynchronous telehealth allows specialists and experts in multiple locations to consult with each other. It is often used in specialties such as dermatology, internal medicine, ophthalmology, and radiology. Hospitals may also use secure telehealth systems to transfer electronic health records to other hospitals and clinics. Remote patient monitoring is often used to monitor vital signs and other critical information during surgery, allowing the surgeon and nursing staff to focus on other critical matters. It can also be used in post-surgical recovery to watch for medication reactions and post-surgical complications.

The rate of telehealth expansion in hospital settings appears to be growing more rapidly than traditional outpatient services.

Medicare and Medicaid Coverage

Medicare and many state Medicaid programs cover telehealth in some form. Medicaid often mirrors Medicare coverage guidance but may be affected by differing state parity laws, which are described below.

Medicare

Medicare has historically covered a limited number of telehealth

services, such as office visits and psychotherapy, but recently increased the number and type of services covered. Medicare's definition of telehealth services can be found in the Code of Federal Regulations (42 CFR 410.78). The Social Security Act dictates what telehealth services are covered under Medicare and includes five primary coverage conditions:

1. The beneficiary (patient) is located in a qualifying rural area
2. The beneficiary is located at one of eight types of qualifying originating sites
3. The services are provided by one of 10 categories of distant site practitioners eligible to furnish and receive Medicare payment for telehealth services
4. The beneficiary and distant site practitioner communicate via an interactive audio and video telecommunications system that permits real-time communication between them and
5. The Current Procedural Terminology/Healthcare Common Procedural Coding System (CPT/HCPCS) code for the service itself is named on the list of covered Medicare telehealth services

Of note are the qualifying originating site requirement and the eligible categories for distant site practitioners. An originating site is the location where the Medicare beneficiary receives the services through a telecommunications system. Generally, the site must be outside a metropolitan area and must qualify as a rural Health Professional Shortage Area (HPSA). These sites can include physician offices, hospitals, rural health clinics, community mental health centers, skilled nursing facilities, and other specified places of care. A distant site practitioner is an individual who can furnish and receive reimbursement for covered telehealth services, subject to state law. These include physicians, physician assistants, nurse practitioners, clinical psychologists, and other health-related professionals.

In 2019, Medicare added stroke assessment and treatment, substance use disorder services, and telehealth services at renal dialysis facilities under certain circumstances. For 2020, the

Centers for Medicare & Medicaid Services (CMS) has indicated that Medicare plans to cover additional office-based treatments for opioid use disorders and expand the ability of Medicare Advantage plans to offer telehealth benefits. The most recent guidance by CMS regarding telehealth coverage by Medicare can be found at https://www.medicare.gov/coverage/telehealth. Another excellent resource is the Medicare Learning Network booklet titled Telehealth Services.

Medicaid Telehealth and Parity Laws

Medicare is not the only program that offers telehealth services. In addition to private health plans, many state Medicaid programs cover telehealth services in some form. Most states currently cover several types of telehealth as cost-effective alternatives to traditional health care. Although billing requirements vary by state, many Medicaid programs have reimbursement policies that are similar to Medicare, including originating site and distant site practitioner requirements. A good reference for Medicaid telehealth services can be located here.

A majority of individual states have also passed parity laws regarding telehealth services. Parity laws usually require health insurers to cover telehealth services comparable to traditional in-person services. However, although many states have coverage rules similar to Medicare, policymakers are currently grappling with the lack of uniformity in individual state parity laws.

Enforcement Matters in Telehealth

New Technology, Same Old Fraud

While telehealth technology may be new, the fraud schemes will sound familiar. The provision of telehealth is not immune to billing for services not rendered, upcoding, misrepresentation, and the kickbacks and bribes that are frequently associated with traditional health care fraud. However, due to the expansion of telehealth in both inpatient and outpatient services and the troublesome combination of telehealth with telemarketing schemes, the Department of Justice (DOJ) and associated enforcement agencies have recently made telehealth a particular area of focus. In addition, even legitimate telehealth companies may encounter cybersecurity incidents that can expose large volumes of sensitive patient data. Several examples are included below.

Remote Patient Monitoring

Remote patient monitoring allows health care professionals to track a patient's vital signs and activities remotely, without the need for a specialist on-site. This is often used in an inpatient setting, such as during surgery or to monitor patients hospitalized in critical care units. It may also be used to monitor high-risk patients, such as those with heart conditions, after surgery and/or hospitalization. In an outpatient setting, it can be used to track patients with quickly fluctuating conditions – such as the glucose levels of patients with labile (hard-to-control) diabetes or fetal heart monitors in premature infants.

Fraud related to remote patient monitoring often consists of misrepresentation and/or billing for services not rendered. The risk to patients in these types of fraud schemes cannot be understated.

Fraud related to remote patient monitoring often consists of misrepresentation and/or billing for services not rendered. The risk to patients in these types of fraud schemes cannot be understated. For example, in October 2015, the DOJ announced that Robert E. Windsor, an Atlanta-area physician, was sentenced to three years in federal prison and ordered to pay over $1.1 million in restitution for billing for surgical monitoring services that he did not perform. Windsor claimed that he had monitored the health of patients during surgery when he actually had an unqualified medical assistant do the work.

In a more recent case in March 2018, the DOJ announced that Marshfield Medical Inc., formerly known as Bromedicon, agreed to pay a False Claims Act settlement of $550,000 for submitting false claims to Medicare and other programs for failing to provide a qualified physician during surgical monitoring. The press release noted that in some cases between 2011 and 2015 the monitoring physician was Bromedicon's medical director, who was a foreign medical school graduate with no license to practice medicine in the United States. In other instances, no one monitored the data stream from the surgeries, including brain and spinal surgeries. Bromedicon violated the False Claims Act by submitting claims for reimbursement as though they were provided by one of the licensed physicians employed by their company.

Telehealth and Telemarketing

In the past few years, the DOJ, the U.S. Department of Health & Human Services (HHS) Office of Inspector General (OIG), and the Federal Bureau of Investigation (FBI) have initiated significant

enforcement action against criminals involved in telemarketing fraud related to health care. Many of these cases also involve telehealth services where a physician or someone falsely representing a provider provide brief phone assessments and video consultations. In many instances, the patient is identified and contacted through a telemarketing scheme – often for durable medical equipment (DME), hospice, or home health services. The criminals use social engineering techniques to convince unsuspecting patients (often vulnerable seniors) that they need a particular service or type of medical equipment. Once they obtain the patients' insurance and other identifying information, they connect them to telehealth physicians under the guise of legitimate services. However, these sham services are far from legitimate and range from medically unnecessary services to medical identity theft. In some cases, the fraudulent telehealth company may lure new, retired, or financially strapped physicians into the scheme. In other instances, a single physician may write hundreds of medically unnecessary prescriptions for lucrative kickbacks.

The criminals use social engineering techniques to convince unsuspecting patients (often vulnerable seniors) that they need a particular service or type of medical equipment. Once they obtain the patients' insurance and other identifying information, they connect them to telehealth physicians under the guise of legitimate services. However, these sham services are far from legitimate and range from medically unnecessary services to medical identity theft.

In an April 2019 enforcement initiative, the DOJ, HHS-OIG, and the FBI announced charges against 24 individuals for over $1.2 billion in losses involving telehealth services for DME. The takedown involved the execution of over 80 search warrants in 17 federal districts and included five telehealth companies and the owners of dozens of DME companies. The scheme purportedly involved the payment of kickbacks by DME companies in exchange for the referral of Medicare beneficiaries by providers. The providers worked for several telehealth companies, including an international telemarketing network that allegedly, according to a Department of Justice press release, "lured over hundreds of thousands of elderly and/or disabled patients into a criminal scheme that crossed borders, involving call centers in the Philippines and throughout Latin America." The telehealth physicians allegedly had only brief telephone conversations with patients they had not seen previously.

Following on the heels of this scam, in September 2019 the DOJ, HHS-OIG, and the FBI initiated a nationwide takedown involving

35 defendants and dozens of telemedicine companies. The case was touted as one of the largest health care fraud schemes ever charged. Among those charged were nine doctors and numerous company executives, including chief executive officers and chief financial officers. The alleged scheme involved the payment of illegal kickbacks and bribes to providers working with fraudulent telehealth companies in exchange for the referral of Medicare beneficiaries to laboratories in order to bill for expensive genetic tests that were medically unnecessary or never provided. The scheme purportedly ensnared elderly and disabled victims into a scheme where the telehealth physicians prescribed expensive genetic tests after a brief telephone conversation or without any patient interaction for patients they never met or had previously treated. The DOJ press release alleges that these companies were responsible for over $2 billion in losses related to fraudulent genetic testing.

Telehealth and Cybersecurity

Another area of telehealth fraud is related to cybersecurity. Cybersecurity concerns and privacy issues are a frequent occurrence with today's rapidly changing digital technology. Even if the proper fraud protections are in place, telehealth is not without risk. For example, digital communication platforms such as Skype and FaceTime may be popular with consumers but are not a wise choice for telehealth applications that contain large volumes of health data. Telehealth companies need to ensure their technology, including systems maintained by third-party administrators, has strong cybersecurity protections in place to defend against unauthorized access and cyberattacks. Numerous breaches of medical data systems have been reported by health care entities and systems over the last few years, and even legitimate telehealth companies may find themselves facing legal scrutiny for failure to protect personal health information.

In August of 2018, a telehealth company in Mexico experienced a data breach of 2.4 million patients in Mexico. The breach purportedly contained insurance information, dates of birth, addresses, disabilities, and other sensitive information. In the United States, the HHS secretary is required by law [Section 13402(e)(4) of the HITECH Act] to post a list of breaches of unsecured protected health information affecting 500 or more

individuals. An updated list of all breaches reported within the last two years is available at https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

Red Flags of Telehealth Fraud

While telehealth schemes may be sophisticated, the red flags of telehealth fraud are simple. Everyone, from beneficiaries to seasoned investigators, should be on the lookout for telehealth services where the online provider, who has never seen the patient previously, aggressively pushes a health care product, such as a wheelchair, or a health care service, such as hospice, on the first and only online visit – with reassurances that insurance will cover the full cost. In addition, telehealth services initiated by robocallers are worthy of significant scrutiny since telemarketing is currently a significant driver of health care fraud and financial/medical identity theft. No one needs to be an expert in technology to protect themselves from telehealth fraud.

No one needs to be an expert in technology to protect themselves from telehealth fraud.

The Future of Telehealth

Is There a Tricorder in Your Future?

Telehealth may be on the rise, but is it here to stay? The general growth in online services of all types and the steady increase in telehealth services being offered by public and private health insurance indicate that future office visits may be online. However, most individuals are still more comfortable discussing their health concerns face-to-face with a provider as opposed to a computer screen. Until Star Trek-style tricorders that sense illnesses without touching a patient are invented, the strong majority of diagnostic laboratory and radiology screenings will still require an individual to be present. While it has yet to be seen whether telehealth is the new office visit, it's a good bet that the old fraud schemes won't be going away anytime soon. Telehealth has the potential to improve access to quality health care and save costs – as long as professionals and consumers stay on guard for fraud, waste, abuse, and cyberthieves.

This article was supported, in part, by grant numbers 90SATC0001 and 90MPRC0001 from the Administration for Community Living (ACL), Department of Health and Human Services, Washington, D.C. 20201.