Telemedicine/Telehealth: Legal, Financial and Practical Issues

Margaret Davino

by Margaret Davino

Technology has become a part of our everyday lives: both personally and in the workforce. One part of technology that the healthcare workforce is experiencing more and more is telemedicine, sometimes called telehealth. Telemedicine is the provision of clinical care to patients from a distance by means of telecommunications technology. Telemedicine allows for more connectivity between health care providers and patients, including by phone, email and webcam, and also allows for provision of quality care in remote places where medical expertise may not otherwise be available.

US News & World Reports' description in August tells the story well: of a retired carpenter, 74, who "these days, even though he suffers from severe chronic obstructive pulmonary disease, doesn't want to go anywhere near a medical facility. And he doesn't need to, even though his COPD has been bad enough in the past to regularly land him in the emergency room and the intensive care unit. The reason: he now gets his care from Mercy Virtual Care Center some 50 miles away. Mercy's providers have been able to detect subtle health shifts in time to avert the cascade of deterioration that put him in the ICU, intervening even before patients experience symptoms. "Mercy Virtual Care's 125,000-square-foot facility" houses more than 300 medical professionals who sit in front of monitors and computer displays, watching over the care of patients at 38 hospitals in seven states. In addition to intensivists who observe patients and direct care at distant ICUs, neurologists provide guidance on stroke treatment to community hospitals. A team of virtual hospitalists orders and reads tests, and nurses field questions about everything from nosebleeds to sinus infections. Mortality in the ICU "is trending 40 percent less than predicted," says Mercy Virtual's president.

Companies have also started offering telehealth directly to patients. For example, Doctor on Demand advertises that for a modest fee, a patient can have a 15 minute online visit: a face-to-face consultation with a doctor through a smart phone, tablet or computer. The on-line doctor can prescribe many medications over the phone, with some exceptions such as controlled substances, certain sedatives, medications that require close monitoring (e.g., methotrexate), or medications that require administration by a healthcare professional.

Telehealth has a number of benefits, including providing access for care for patients in remote regions of our country and the world, the ability to bring in specialty consults for difficult diagnoses or cases, cost savings for hospitals to provide monitoring of critical patients in their ICUs remotely rather than having an intensivist constantly on site, and the quality benefits of the ability for radiology films to be read 24/7, rather than waiting for radiologists to come in. However, there are downsides as well, including ensuring that information from telemedicine practitioners is communicated to a patient's primary care provider so that the primary care provider is aware and can provide continuity of care; the risk that protected health information may be accessed electronically given the dependence on electronic means of transmission; and the risk that a medical error will occur if there are signs and symptoms that can be elicited only by seeing the patient in person.

There are three types of telehealth: 1) store and forward (where medical data such as radiology images are acquired and transmitted to specialists for assessment at a convenient later time), 2) remote monitoring (where health professionals monitor a patient remotely using various technology), and 3) real-time interactive telehealth (where a patient is seen through video or other conferencing by the healthcare provider in real time). It is important to know the distinction between the different types of telehealth because some states or payers allow or pay for only one type of telehealth.

Although telehealth is growing, and being used in schools, assisted living centers and for remote chronic disease management, one of the biggest challenges to further growth is reimbursement. Some of the commercial telehealth services (e.g., those that offer telehealth doctor appointments) are private pay. Although some patients are willing to private pay for the convenience, telehealth's market will not be fully realized until its services are reimbursed similar to in-person services. Twenty-four states now have "parity" laws, prohibiting health

continued on page 20

continued from page 19

insurers to cover and pay for services via telehealth in the same way as for services provided in person. One of the most recent is New York, which effective January 1, 2016, requires commercial health insurers from excluding from coverage services that are otherwise covered in-person. New York's Department of Health as of the time of this article has not yet published regulations, so this law has not been fully implemented, but provides parity for services of not just physicians, but also physician assistants, dentists, nurse practitioners, podiatrists, optometrists, psychologists, social workers, speech language pathologists, midwives, diabetes educators, asthma educators, genetic counselors, hospitals, home care agencies, hospices, and "any other provider as determined" by the Commissioner of Health pursuant to regulation. New Jersey and Pennsylvania both have legislation pending to expand payment for telemedicine, but nothing has passed as of the date of this writing.

Medicare's reimbursement for telemedicine is still limited. It reimburses for telehealth services in rural areas only, and only for real-time interactive telehealth. If in a rural area, providers eligible for reimbursement under Medicare include physicians, nurse practitioners, physicians' assistants, clinical nurse specialists, nurse midwives, clinical psychologists, clinical social workers, and registered dieticians or nutrition professionals. Medicare has a specific list of CPT and HCPCS codes that are covered for telemedicine services, and the provider must use a GT modifier to show that the service was provided virtually.

Medicaid programs often offer broader coverage of telemedicine, with almost all state Medicaid programs offering reimbursement for telemedicine over live video, but a far smaller number of states covering remote patient monitoring. New Jersey Medicaid currently covers only telepsychiatry services by a psychiatrist or psychiatric advance nurse practitioner, and the patient must be in a mental health clinic or hospital, with the telepsychiatry used to meet the hospital or clinic's requirements for intake evaluations periodic psychiatric evaluations, medication management and/or psychotherapy sessions. Pennsylvania's Medicaid coverage of telemedicine is somewhat broader; it reimburses for live video for (i) specialty consultations by physicians, nurse practitioners or nurse midwives, and (ii) telepsychiatry outpatient services. On the other hand, under New York's new law, as of 2016, New York Medicaid now reimburses for real-time two-way AV communications, store and forward technology, and remote patient monitoring. The patient must be located at a hospital, hospice, mental health facility, diagnostic and treatment center, certain FQHCs, certain school based health centers, and physician offices. New York Medicaid also covers remote patient monitoring in a patient's home.

Telehealth also brings with it a number of legal issues, including the following:

1. Licensing limitations

The location of a patient is considered to be the "place of service" of that patient, and the healthcare provider must comply with the laws of the state where the patient sits. With some exceptions (e.g., physician-to-physician consultations, or physicians licensed in a "border state"), the practitioner must be licensed in the state in which the patient sits.

This sometimes can cause wrinkles in care. For example, at Mayo Clinic, doctors who treat out-of-state patients can follow up with patients via phone, email or web when they return home, but they can only treat the conditions treated in person. If a patient has a new problem, the patient may be referred to his or her primary care practitioner licensed in the patient's state to discuss that issue.

Some sites may not consider certain services to be "practicing medicine" or another profession. For example, FirstDerm users upload photos and a description of skin issues, and a dermatologist (most of whom are in Europe) replies within twenty-four hours with a possible identification of the issue and options. FirstDerm states that no patient relationship exists in this situation because both the patient and physician are anonymous to the other.

2. HIPAA and patient confidentiality laws

All healthcare providers must comply with applicable patient confidentiality laws, including state law and HIPAA. Although most healthcare providers are "covered entities" under HIPAA, a provider (whether telehealth or not) is a covered entity under HIPAA only if it bills electronically for services using any of the HIPAA transaction code sets. A provider must meet applicable confidentiality laws whether the services are provided in-person, or through telehealth. If HIPAA is involved, this requires that both the HIPAA privacy and security rules are complied with. HIPAA privacy regulations require policies and procedures as to maintenance of protected health information, and training of personnel – both at the originating site (where the patient sits) and at the distant site (where the provider sits). HIPAA security rules require that any electronic protected health information be secure, whether that data is stored, used or transmitted. A healthcare provider must start with a security risk assessment to determine how electronic protected health information is being used, where it is stored, and how the technology used for telehealth is able to ensure high-level security and prevent breaches of patient information.

Because telehealth involves sharing of information, patient confidentiality/HIPAA concerns include looking at who else can access that protected health information. A vendor or person acting on behalf of the healthcare provider who can access that information is considered to be a "business associate"

under HIPAA, and the provider must put a business associate agreement in place. Because HIPAA covers protected heath information no matter how far down the line the information is shared, business associates must also have agreements in place with their subcontractors to protect the information. In addition, healthcare providers should look at any party with whom protected health information is shared, to address questions about shared responsibility for managing and securing patient information generated through a telehealth encounter.

HIPAA to-dos with telehealth include:

(i) ensuring secure communications channels
(ii) implementing business associate agreements and other confidentiality and privacy agreements
(iii) providing education regarding appropriate use of tele health technologies
(iv) understanding how and what patient information is being collected and stored
(v) performing a HIPAA security risk analysis
(vi) ensuring that all subcontractors with access to protected health information comply with HIPAA requirements.

3. Malpractice liability

Health professionals who provide services via telehealth have the same duty of care to a patient as a healthcare professional providing services in person. This is recognized in some of the publications of the various medical and other professional boards that have reviewed telemedicine practices, including the AMA Telemedicine Policy. Fortunately for telehealth providers, lawsuits to date have not been common. According to a publication by Willis Towers Watson, most involve teleradiology, e.g., a failure to diagnose properly.

Healthcare providers involved with telehealth must ensure that they are covered under their malpractice insurance policy. Although telehealth has not had a lot of claims, some insurers provide coverage only in a particular state, so providers must ensure that their insurance carriers are aware of their telemedicine activities and agree to provide coverage for claims by patients in other states.

4. Credentialing and privileging

Hospitals and other facilities require that providers practicing at those facilities be "credentialed" or "privileged" after a review of those practitioners' background, experience and credentials. The need to credential practitioners caring for a facility's patients applies whether the practitioners are on-site or remote, e.g., radiologists reading scans for hospital patients off-site.

The Joint Commission has allowed hospitals to "privilege by proxy," i.e., accept a distant site hospital's credentialing and privileging decisions, so that hospitals are not required to undergo a separate privileging and credentialing process for each practitioner providing telehealth services from a distant site.

Effective July 5, 2011, the Centers for Medicare and Medicaid Services (CMS) changed their conditions of participation for hospitals to also allow credentialing by proxy, if the following conditions are met:

- the distant site hospital must participate in Medicare or be a telemedicine entity
- provider is privileged at the distant site hospital
- a current list of the telehealth provider's privileges is given to the originating site hospital
- a written agreement between the parties
- the telehealth provider is licensed in originating site hospital's state
- originating site hospital reviews provider and shares info with distant site hospital
- sites aware of all adverse events

Therefore, hospitals may now perform credentialing by proxy of telehealth practitioners under Medicare conditions of participation. However, the hospital's bylaws must allow "remote credentialing," and such must also be permitted by State law. For example, the Pennsylvania Department of Health published a "Telemedicine Survey Guidelines and Department of Health Survey Policy" dated April 25, 2013, that gave guidance as follows:

"The originating site hospital may, but not must, accept the provider credentialing of the distant-site hospital specific to the medical discipline in which the provider is practicing telemedicine. Originating site hospitals need only demonstrate verification of provider credentials issued by the distant-site hospital, including verification that each practitioner has sufficient raining the specified medical discipline in which he or she is practicing telemedicine. The distant site facility shall determine "sufficient" training for providers of telemedicine services.

5. Prescribing medications

There has been concern for some time that practitioners may be financially induced to write prescriptions for persons who fill out questionnaires on the web, with no physical exam and sometimes without knowing anything about the "patient's" medical history. This concern is recognized by the Federation of State Medical Boards (FSMB)'s Model Policy for the Appropriate Use of Telemedicine Technologies in the Practice of Medicine, which emphasizes the importance of a physician-patient relationship before telemedicine services, particularly prescribing. The FSMB Policy states that "Telemedicine technologies, where prescribing may be contemplated, must implement measures to uphold patient safety in the absence of traditional physical examination. Such measures should guarantee that the identity of the patient and provider is clearly

continued on page 22

continued from page 21

established and that detailed documentation for the clinical evaluation and resulting prescription is both enforced and independently kept. Measures to assure informed, accurate, and error prevention prescribing practices (e.g. integration with e-Prescription systems) are encouraged. "

Special attention must be given to the prescribing of controlled substances. The Ryan Haight Online Pharmacy Consumer Protection Act, named for an 18-year-old who died after overdosing on a prescription painkiller he obtained on the Internet from a medical doctor he never saw, was enacted on October 15, 2008 and requires at least one in-person medical evaluation before a controlled substance may be prescribed. It amended Section 309 of the Controlled Substances Act (21 U.S.C. 829) to state that "No controlled substance that is a prescription drug as determined under the Federal Food, Drug, and Cosmetic Act may be delivered, distributed, or dispensed by means of the Internet without a valid prescription." The term valid prescription means a prescription that is issued for a legitimate medical purpose in the usual course of professional practice by either a practitioner who has conducted at least one in-person medical evaluation of the patient; or a covering practitioner.

The term in-person medical evaluation means a medical evaluation that is conducted with the patient in the physical presence of the practitioner, without regard to whether portions of the evaluation are conducted by other health professionals. However, the law specifically states that "Nothing in this subsection shall apply to the delivery, distribution, or dispensing of a controlled substance by a practitioner engaged in the practice of telemedicine."

Consistent with the Controlled Substances Act (CSA) itself, the Ryan Haight Act relates solely to controlled substances, specifically, those psychoactive drugs and other substances–including narcotics, stimulants, depressants, hallucinogens, and anabolic steroids–that are placed in one of the five schedules of the CSA due to their potential for abuse and likelihood that they may cause psychological or physical dependence when abused. Controlled substances constitute approximately 10 percent of all drug prescriptions written in the United States.

6. Informed Consent

Informed consent from patients in a telehealth setting requires special thought because of the fact that, in addition to the information provided regarding patient care, the provider must also consider consent for the use of technology, any limitations from use of technology, and any sharing of information expected. The Federation of State Medical Board recommends that evidence documenting appropriate patient informed consent for the use of telemedicine technologies be obtained and maintained, and as a baseline, include the following terms:

- Identification of the patient, the physician and the physician's credentials;
- Types of transmissions permitted using telemedicine technologies (e.g. prescription refills, appointment scheduling, patient education, etc.);
- The patient agrees that the physician determines whether or not the condition being diagnosed and/or treated is appropriate for a telemedicine encounter;
- Details on security measures taken with the use of telemedicine technologies, such as encrypting data, password protected screen savers and data files, or utilizing other reliable authentication techniques, as well as potential risks to privacy notwithstanding such measures;
- A hold harmless clause for information lost due to technical failures; and
- Requirement for express patient consent to forward patient-identifiable information to a third party

In addition, thought must be given to how informed consent is documented and maintained in the medical record, so that not only is the patient truly aware of the issues with regards to telehealth, but that documentation exists of the patient's consent to proceed after knowledge of the risks, benefits and alternatives.

7. Medical Devices

Telehealth providers need to consider whether the technology used may be considered to be a "medical device," and whether such has been approved by the Food and Drug Administration (FDA). When equipment or software is intended for use in the diagnosis or treatment of a disease or other condition, the FDA considers it to be a medical device. This may involve registration and listing, premarket notification or approval, use of good manufacturing practices, and post-market surveillance. In September 2015, the FDA published "Mobile Medical Applications: Guidance for Industry and Food and Drug Administration Staff." This Guidance recognized that not all mobile apps are medical devices, and therefore the FDA does not regulate them. Some mobile apps may meet the definition of a medical device, but because they pose a lower risk to the public, the FDA intends to exercise enforcement discretion over these devices (meaning it will not enforce requirements under the Food Drug & Cosmetic Act). The FDA stated that it intends to apply its regulatory oversight to only those mobile apps that are medical devices and whose functionality could pose a risk to a patient's safety if the mobile app were to not function as intended.

In addition, the FDA just issued October 14, 2016 draft guidance titled "Software as a Medical Device: Clinical Evaluation." This draft guidance defines Sofware as a Medical Device

(SaMD) as "software intended to be used for one or more medical purposes that perform these purposes without being part of a hardware medical device." It specifically includes mobile apps and in-vitro diagnostic (IVD) medical devices, but states that software does not meet the definition of SaMD if its intended purpose is to drive a hardware medical device. For example, software that allows a commercially available smartphone to view images for diagnostic purposes obtained from an MRI scan; or processes images from hardware medical devices for aiding in the detection of breast cancer is considered to be SaMD.

7. Fraud and abuse (anti-kickback) laws

The federal anti-kickback law prohibits offering, paying, solicit or receiving remuneration to induce referral of items that are paid for by Medicare, Medicaid or any other federally funded healthcare program. This issue may arise if telehealth equipment is being leased from a physician or other entity referring business to the telehealth provider. There are a number of "safe harbors" under the anti-kickback law, allowing transactions such as employment, personal services arrangements, leases, etc., to go forward without violation of the anti-kickback law, but specific requirements must be included in a transaction and written agreement to fall within the protection of a safe harbor and avoid potential prosecution under the anti-kickback laws.

AMA Telemedicine Policy

Many of the above issues are set forth and explained in the Telemedicine Policy published by the American Medical Association. Although applicable only to physicians, and not legally binding, the AMA's Telemedicine Policy provides an excellent overview of how State Boards of Medicine may view telemedicine practices, and a good structure as to how to develop telehealth programs. Below is a summary of many of the principles set forth in the AMA Telemedicine Policy:

1. Establish patient relationship before provision of telemedicine services, through:
   - A face to face exam, if this would be required for the same service provided in a non-telemedicine context
   - Consultation with a physician with an ongoing patient relationship who agrees to supervise patient's care, or
   - Meeting evidence-based clinical practice guidelines developed by specialty societies, e.g., radiology

The AMA recognizes that certain exceptions exist as to the above, e.g., on-call arrangements, cross-coverage, and emergency situations.

2. Abide by state licensure laws and practice laws.
3. Patients must have a choice of providers.
4. Patients must have access to the qualifications of the provider(s) that they will see in advance of the visit.
5. The standards and scope of services provided through telemedicine are consistent with in-person services.
6. Evidence-based guidelines should be followed.
7. Patients must know the costs and any limitations of telehealth, e.g., if there are limited medications available.
8. The patient's medical history must be collected.
9. Services must be properly documented.
10. Care coordination with patient's existing treating physicians should occur.
11. Protocols should exist for referrals for emergencies.
12. Laws for privacy and security of patient medical information must be abided by.
13. Physicians are responsible for supervision of non-physician providers, including:
    - protocols, conferencing & record review
    - visit sites & know competence of providers
    - conformance to state practice acts

Conclusion

Telemedicine certainly is going to expand in the future. Even with the change of administration in the federal government, states are increasingly adopting laws allowing telemedicine to keep up with the increasing use of such. In addition, telemedicine may be used more as accountable care organizations (ACOs) look at how to best provide for care management of their patients to avoid hospital readmissions. All providers should be aware of the issues with telehealth and its use in the future.

References

Federal of State Medical Boards: "Model Policy for the Appropriate Use of Telemedicine Technologies in the Practice of Medicine," April 2014.

American Medical Association: AMA Telemedicine Policy, 2015

About the author

Former general counsel to medical centers in New York and New Jersey, Margaret is an experienced health care attorney at the national law firm of Fox Rothschild LLP. She handles a broad spectrum of health care matters, including transactional, compliance, contractual, corporate, regulatory, governance, managed care/payer (including value-based arrangements) and risk management issues. Her clients include hospitals, physicians and physician groups, ACOs, startup companies, FQHCs, home care agencies, pharmacies, laboratories, agencies for the developmentally disabled, care management companies, billing companies, nonprofit companies, health care IT vendors and a variety of other providers and entities in the health care space. She can be reached at mdavino@foxrothschild.com.