Telemedicine: A Virtual Compliance Jigsaw Puzzle

Michael J. Sacopulos, CEO, Medical Risk Institute and General Counsel, Medical Justice Services

Telemedicine is a hot topic across the country. Earlier this year, Forbes proclaimed "Telemedicine may just be the biggest trend in digital health in 2015." New services, such as Zwivel are coming online with increasing frequency. From physicians to administrators to patients, everyone seems to be interested in the possibilities of telemedicine.

Perhaps we should not be surprised by this trend. High speed internet connections are now the norm. Services like Facetime and Skype are more popular than ever. Under continued pressure to cut costs and cope with declining reimbursements, administrators believe telemedicine offers a tool for increasing efficiency. Patients too like the convenience and increased options that flow from telemedicine. So what's not to like? Shouldn't we embrace the "new normal" and sign on to a great, brave new world?

Maybe, first let's proceed with caution. There are a number of state and federal requirements that must be complied with when you take your practice on line. Here are some things to consider:

Licensure

Medical providers "must be licensed by, or under the jurisdiction of, the Medical Board of the State *where the patient* is located," according to the Federation of State Medical Boards' Model Policy for the Appropriate Use of Telemedicine Technologies in the Practice of Medicine. Unfortunately, this requirement imposes traditional state boundaries on the cyber world. Efforts need to be made to identify the residences of prospective telemedicine patients so the medical provider does not accidentally practice in a state without a license.

Professional Liability Considerations

Most professional liability insurance policies provide state specific coverage. This means that should a provider accidentally practice telemedicine on an out of state patient, there may be no coverage. Providers wanting to expand into the area of telemedicine should check with their insurance carrier.

Another consideration relates to cyber issues. Traditional medical malpractice policies provide little to no coverage for electronic breaches. The nature of a telemedicine generates exposures to a variety of cyber risks. Any practice moving forward with offering telemedicine should have a comprehensive cyber insurance policy.

Standard of Care

Telemedicine is the practice of medicine. It is not some lite version of medicine. All the duties and obligations that come with in person consultations are owed to the remote telemedicine patient. As the American Medical Association stated recently "… there is a general consensus (one that the AMA supports) that care provided via telemedicine needs to meet the same standard as care provided in person …" The Federation of State Medical Boards made clear the position by stating, "In fact, these guidelines support a consistent standard of care and scope of practice notwithstanding the delivery tool or business method in enabling physician-to-patient communications."

Before starting to use telemedicine as a tool to consult with remote patients, a practice should plan how it will meet the standard of care it provides for its in-office patients. For example, how will it document a dermatological condition? If the condition is normally photographed when a patient is in the office, then the practice should be ready to capture the same quality of image via telemedicine. Each step of the consultation should be planned in advance to ensure it is equal in quality to an in-office evaluation.

Patient Privacy

Any form of electronic communication with a patient should immediately bring to mind HIPAA and HITECH Act obligations. Whether the electronic connection with the patient is via email, text messaging, or video conference, the platform should be secure. Private and confidential patient information is being transmitted and the patient has a legal right to protect the information in transit.

The Federation of State and Board Telemedicine Guidelines specifically state "Physicians should meet or exceed applicable federal and state requirements of medical/health information privacy, including compliance with the Health Insurance Portability and Accountability Act (HIPAA) and state privacy, confidentiality, security, and medical retention rules." The FSMB Guidelines go on to suggest that written policies should be maintained to address one: (1) privacy; (2) healthcare personnel who will be processing messages and patient communications; (3) hours of operations; (4) types of transactions that will be permitted electronically; (5) required patient information to be included in the communication, such as patient's name, identification number and type of transaction; (6) archival and retrieval; and (7) quality oversight mechanisms. Finally, telemedicine practitioners are cautioned to periodically evaluate their policies and procedures to insure that they are current and are readily accessible. Finally, FSMB informs us that the electronic communications received patients must be maintained within secured technology "password protected encrypted electronic prescriptions, or other reliable authentication and techniques."

It is reasonable to assume that additional patient privacy requirements will be coming in the near future. This well may be in reaction to large scale breaches such as Anthem Insurance experienced earlier this year. Studies show that medical identity theft grew at an alarming rate in

2014. Government officials including the FBI and California Attorney General have specifically cautioned medical providers that their patients' electronic data is at risk for hacking and theft. All of this should serve as a warning to telemedicine providers to comply with existing state and federal regulations. Telemedicine providers should also anticipate increasing privacy standards in the future.

Informed Consent

Before practicing telemedicine, a medical provider should obtain appropriate informed consent from his or her patient. The informed consent document should: (1) clearly state the patient's identity; (2) clearly state the physician's identity and qualifications; (3) specify the scope of activities that the practice will be using telemedicine technologies to fulfill (for example, patient education, prescription refills, scheduling appointments, etc.,); (4) patient must acknowledge that it is within the medical provider's sole discretion to determine if the available telemedicine technologies are adequate to diagnose and/or treat the patient; (5) patient should acknowledge the possibility of, and hold harmless the medical provider for any technology failures and/or interruptions; (6) the practice should, as part of the informed consent process, provide information on the telemedicine technologies privacy and security standards (for example, the inscription of data, firewalls, etc.); and (7) finally, the informed consent document should specify express patient consent to forward patient information to a third party if necessary.

Referrals for Emergency Service

The FSMB suggests that telemedicine practitioners have a written protocol in the event that a remote patient needs emergency services. This emergency protocol should cover possible

scenarios when patients require acute care. How and where referrals are to be made should be covered in this protocol.

State Specific Requirements

The scope of permissible telemedicine varies significantly by state. Some states specifically require that a physician/patient relationship only be established in a person with an exam and diagnosis and treatment plan including prescriptions. The relationship may thereafter be conducted through telemedicine. That is the established regulation in the State of New Hampshire, and other states follow similar procedures. While Idaho does not have specific telemedicine laws, it has recently disciplined a physician for prescribing antibiotics over the phone without having first examined the patient in person. Other states, including New Mexico, take a more liberal stance on telemedicine. In New Mexico physicians are allowed to establish a patient/physician relationship and issue prescriptions based upon telemedicine interaction with patients.

Telemedicine is receiving much attention at the moment. The American Medical Association is in the process of adopting a Code of Ethics for physicians who provide clinical services through telemedicine. Texas has recently issued new telemedicine guidelines to its practitioners. All of this should serve as a warning to those interested in telemedicine to consult with their State Board of Medicine before engaging in telemedicine activities.

Your Telemedicine Checklist

Telemedicine offers opportunities for both providers and patients. Those wishing to electronically interact with patients should first work their way through the checklist below:

(1) Examine the electronic ways your practice and patients communicate. From patients portals to staff testing, you need a complete picture of your electronic communications before engaging in telemedicine;

(2) Make sure that your forms of electronic patient communications are HIPAA compliant and secure;

(3) The internet may know no bounds, but your license does. Be careful not to provide medical services to individuals that live in states where you are not licensed;

(4) Check with your State Board of Medicine to determine what your state's specific telemedicine limitations include;

(5) Develop a specific informed consent document that complies with your state's requirements as well as the Federation of State Medical Board's suggestions;

(6) Develop a list of disclosures to provide to prospective patients before they engage you for telemedicine services; and

(7) Make sure that you are adequately insured. This means check with your professional liability carrier and get a cyber insurance policy.

With advanced planning and a little effort, you will be able to make your way through the compliance requirements to practice telemedicine. With careful planning, both you and your patients will enjoy the benefits of a telemedicine practice.

Michael J. Sacopulos is the CEO of Medical Risk Institute (MRI) and serves as General Counsel for Medical Justice Services, a 4,000 member group with physicians in all 50 states. Medical Risk Institute provides proactive counsel to the healthcare community to identify where liability risks originate, and to reduce or remove these risks. In 2012, Michael won the Edward B. Stevens Article of the Year Award for MGMA and had a Top 10 article of 2014 on Medscape. He has recently been named the Executive Vice President of the Aesthetic Stem Cell Society. Additionally he has written for the Wall Street Journal, Forbes, Bloomberg and many other publications for the medical profession. He is a frequent national speaker and has appeared on Fox Business News.

He attended Harvard College, London School of Economics and Indiana University/Purdue University School of Law. He may be reached at msacopulos@medriskinstitute.com.

Originally in July/August 2015.

Tagged: Healthcare & Legal