

Managing the risks of practicing telemedicine

by Eric Berkman

Published: December 27, 2010



Telemedicine - the practice of physicians using technology to consult remotely with patients or other doctors - is a growing field that has the potential to reduce health care costs while making it more convenient to treat patients who cannot easily access the right doctor in person.

But legal and medical experts say that any physician or medical group that considers adapting telemedicine in a practice must be aware of possible liability traps and know how to manage the risks.

Telemedicine comes in a variety of forms, ranging from videoconferencing and communication over customized Internet channels to good old-fashioned telephone and e-mail contact. (See "Advice for old-fashioned telephone use" on page 16.)

And it offers plenty of benefits.

"It has a lot of potential for managing chronic diseases," such as diabetes or hypertension, said Kevin M. Pho, a Nashua, N.H., internist and publisher of KevinMD.com, one of the most widely read medical-affairs blogs. "These aren't conditions where you necessarily have to see a patient face-to-face all the time, and you can do a lot of patient management via videoconference, the phone or e-mail."

It's also useful for patients who are homebound because of health issues or live in remote locations hundreds of miles from a specialist or even a doctor, said Roy Schoenberg, chief executive officer of American Well Systems in Boston, which produces customized Internet platforms that enable patients (and doctors) to connect with a physician on demand.

"This is a completely new way of doing health care," said Schoenberg, who is a physician himself. "It really doesn't matter whether you're in downtown Boston or in rural Maine surrounded by snow and ice. You have immediate access to the same health care professionals."

Observers expect the field to explode once Medicare and more insurers begin reimbursing for services that aren't conducted in person.

Even if reimbursement doesn't happen, anyone who delves into telemedicine needs to be sure to address areas of potential risk, said Anne Huben-Kearney, vice president of risk management at ProMutual Group, the commonwealth's biggest medical liability insurer.

Here are six areas that physicians engaging in telemedicine should address:

- **Privacy, security and patient confidentiality**

Privacy and security are the two biggest telemedicine-related concerns for professional liability insurers and patients, says Huben-Kearney.

Patients need to be assured that whatever personal medical information they're transmitting is going to the right person, she said.

"I think people are concerned that their information is going to be hacked," said Huben-Kearney.

An important place to start is by ensuring that the patient and physician each have a unique, secure password to link up.

"Otherwise, you don't know who you're actually talking to," she said. "It could be anyone using a patient's name going onto the site saying, 'I have these questions and concerns.' So we like to see passwords that aren't shared with anyone."

If your group practice implements an Internet-based telehealth platform, the vendor should set it up so that doctors have to be on a list of approved providers within the group to sign up, said Schoenberg.

He said there also needs to be a security infrastructure that ensures all live communication is completely encrypted.

"The storage of any information generated must be accessible only to the actual patient and physician," not even to the vendor or system operator, Schoenberg added. "It must be encrypted at the database level."

It's also critical to remember that patient confidentiality regulations like HIPAA apply regardless of whether the communication takes place in person or via technology, said David Harlow, a health care lawyer and consultant in Newton, Mass. and author of HeathBlawg, a health law and policy blog.

In fact, Harlow pointed out that amendments to HIPAA under the HITECH Act impose additional requirements on business associates of health care providers, including telemedicine vendors.

"It's no longer sufficient to get a vendor to say, 'I understand the requirements and will keep information private,'" said Harlow. "There's an affirmative obligation on the health care provider to be responsible for the privacy and security operations of the vendor."

In addition, any practice using telemedicine tools needs to update its HIPAA privacy notice to address how it protects privacy when engaging in telemedicine, Harlow advised.

- ***Informed consent***

Huben-Kearney said that any Internet-based telemedicine site should be up front with the patient about the limitations of the technology - particularly its security - and have the patient sign off on that.

"Patients need to be informed. They're making a decision to participate, but they need to be made aware of the potential risks," she said.

Any informed consent form should include the patient's responsibility to use the technology appropriately (for example, don't use the Internet to report a medical emergency); should inform the patient that any messaging platform might only be checked on, say, a daily basis; and that there is no sharing of passwords.

- ***Maintaining continuity of care***

Pho said he hasn't used telemedicine technology such as videoconferencing or communication over customized Internet platforms. But he is a heavy user of social media tools and says many of the risks are the same - particularly when it comes to continuity of care.

"The biggest risks occur when encounters aren't documented," he said. "With a Skype call, a videochat or even a phone call, everything must be appropriately recorded in the chart."

Harlow agreed.

"You want to ensure continuity of care by ensuring all records of patient encounters end up in the same place easily," he said. "[Remote consultations] can end up in the same place, but that can often mean double or triple the work for the physician."

Huben-Kearney added that ProMutual likes to see proof of informed consent scanned into the

record.

- ***Staying in state***

Some Internet-based telehealth involves patients logging onto a secure website and, after providing the relevant information, being connected online with a doctor whom the patient does not know, but who practices in the necessary specialty.

If you're the doctor who has volunteered to consult with individuals at one of these sites, said Harlow, you need to make sure you're only providing services to patients in the state where you're licensed.

"It goes by where the patient is, not by where the doctor is," he said. "A company like American Well would presumably only connect a Massachusetts patient with a Massachusetts doctor, and some states have limited licensure for telemedicine - sort of a separate category of licensure - but most states do not."

Any doctor who is not careful about this issue risks an action by the Board of Registration in Medicine for the unlicensed practice of medicine, Harlow added.

- ***Ensuring the reliability of the technology***

Harlow said that the technology itself can be a liability concern.

For example, what if the connection cuts out at a key moment in the conversation where a doctor is telling a patient to be sure not to take the prescribed medicine with food? Now a technical glitch has resulted in a transmission of inaccurate medical advice.

"If that results in an injury to the patient and there's a lawsuit, who's liable?" asked Harlow. "The standard contract from the technology vendor would say they disclaim all liability. This is something to be aware of."

Of course, depending on the bargaining strength of a physician group versus the tech company, everything is negotiable.

"So this kind of issue would militate in favor of a physician signing up with a larger group. ... By being part of an organization you get better leverage in the negotiation with the vendor," said Harlow.

It's best to try to avoid technical glitches altogether, said Huben-Kearney, which means selecting a competent vendor. Since most physicians and small group practices lack the level of technical expertise to do this effectively on their own, she suggested they contact their liability insurer for advice.

- ***Choosing the appropriate clinical context***

Telemedicine is effective in two major areas of health care delivery, according to Schoenberg.

The first context is acute primary care - emergent issues where patients need timely care, such as bronchitis, urinary tract infections and gastrointestinal infections.

"Usually they're sick and going to see a doctor is difficult," he said. "Or their child is sick at 11 at night and they don't know if they need to go to the emergency room. A telehealth system allows them to bring up a live doctor to make that decision with them."

The other scenario is patients with a chronic condition where the doctor is not establishing a diagnosis, but the condition requires complex daily management.

"Either they can't wait to get to a doctor or it's very difficult for them to show up in the office with the frequency their condition requires," Schoenberg said. "[Telemedicine] allows doctors to be more balanced with how they're treating complex conditions. Diabetes, asthma and heart patients use these systems extensively."

But anything that has to do with trauma or requires a physician to give surgical rather than medical advice is completely inappropriate, he said. Additionally, escalating medical conditions such as chest pains and very high fevers should be dealt with in person.

"In all these cases, even if patients are presenting on our system with these kinds of conditions, the physician will instantly tell them to go the emergency room to be seen physically by a physician," said Schoenberg. **MMLR**

Questions or comments can be directed to the editor at: reni.gertner@mamedicallaw.com

Read more about telemedicine: [Telemedicine as usual: advice for old-fashioned phone use](#)

Complete URL: <http://mamedicallaw.com/blog/2010/12/27/managing-the-risks-of-practicing-telemedicine/>