Just like physicians working with historical and established medical care, all telehealth, video, m-health, and e-health physicians or caregivers must uphold the same standard for safeguarding all of the records on patients’ care and on conversations securely and confidentially. The storage of electronic documents—electronic health records, discussions via telemedicine, photographs, audio, and video recordings (media), etc., must be afforded the same protections and care that are provided for all paper documents. The responsibility has not changed; the media and mode have.

The issues regarding privacy and confidentiality in the medical field are not necessarily any different in an “electronic” environment. Nonetheless, some patients might feel skeptical about the use of or the idea of video, m-health, telehealth, or e-health with its lack of visual prompts or cues. Before proceeding toward an all-electronic communication system, first and foremost, you must verify that the service that you have or the vendor you are investigating has received its HITECH (health information technology for economic and clinical health) certification, that it is compliant with HIPAA (Health Insurance Portability and Accountability Act, 1996), and that you have a current signed business associate agreement (BAA) on file. In addition, you must have on file a current signed patient/provider consent/agreement for telehealth, m-health, e-health, and/or video services prior to proceeding.

We must also acknowledge and respect that there may be an element of cultural diversity involved; we must set ground rules up front; we must watch for facial expressions, and it is essential to listen for frustration and watch for gestures and body language. However, when performing this patient “electronic” evaluation, if your gut instinct tells you to offer the patient a true face-to-face and in-office visit—then go with your gut instinct. This is your intuition telling you something!

In addition, patients may have fears about electronic systems and their reliability, and also about the technology used and the potential for a devastating loss of their protected health information (PHI): chart notes, video etc. Uncertainties about these issues may leave some patients distrustful of any form of e-health, m-health, or telehealth.

Encryption and other concerns

As with any unencrypted PHI, when “video” travels over the “public switched telephone network (PSTN)” without encryption, there is an opportunity for hacking and/or breaches. When investigating services and securing a dedicated pipeline we must verify that the service is using at a minimum Advanced Encryption Standards and that it is operating within a current and up-to-date computer virus security software environment. Having these safeguards may reduce the opportunity for hacking attempts and potential breaches, and may also help to put the patient at ease.

Several of these concerns about technology or services can be addressed through a combination of technical and security measures, such as the enforcement of the privacy rule within the scope of HIPAA, the HITECH regulations, and through California AB-415 (other states may have additional regulatory requirements). It is advised that you check with your appropriate county, state,
or federal agencies in addition to your medical professional liability provider when considering any new technology or services.

There are certain video services such as Skype that have current issues with security and privacy that are known to the industry. At this time, this particular service from Microsoft fails to offer a BAA “which upholds the HIPAA privacy rules,” and it has failed to receive any HIPAA security certifications. The failure to have HIPAA/security measures in place means that there is some potential for a hacking attempt and security breaches. The HIPAA privacy rule specifies “Protected Health Information (PHI) means ‘individually identifiable health information—transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium.’” And therefore such information must be in compliance with the privacy rules (see https://www.federalregister.gov).

At present, in the U.S. there are several secure video conference and telemedicine services or service providers available. It is recommended when moving toward this type of medium that the physician or administrator quality-check each service prior to entering into a contract. When investigating, have a matrix of questions and a place for each vendor’s reply to each query. This matrix should include space for responses about the specific needs of your offices; ask pointed questions about how these service providers or vendors will relate to your business; ask each vendor the same question(s), and remember that the failure to do so may place you and your patients at risk for breaches and your practice for violations if you fail to do this homework.

It is also suggested that your business attorney be in the loop before you contract with any vendor or service. If a vendor or service has not complied with one or more of the security and governmental regulations, that is a red flag! Ask questions like this: “How will your service integrate with my practice management or electronic medical records system?” (These tele-notes or video-chats need to be included in the patient record.) Ask other specific questions as well: Where is the data backed-up? Is it stored within your state, or in mainland U.S.? Who actually owns the data? After your evaluation of each vendor, investigate any specific rules and regulations that are in effect in your state. Will you need additional coverage from your medical professional liability (MPL) company? Does your MPL coverage cross state lines (if the vendor is not in your state)? Remember to secure a BAA, support the HITECH agreement, and be HIPAA compliant in addition to managing and getting a specific patient consent(s) for using telehealth, e-health and m-health services.

All of these considerations should be paramount when moving forward in offering any new services.

Remember that caution and security should always be the first thing you think of when contemplating any video, e-health, m-health, or telehealth services. Familiarizing yourself with the HIPAA privacy rule, the HITECH agreement, the Omnibus regulations, and your state and federal requirements in addition to exploring your MPL limits and the wording in your MPL policies is a must. Instituting a quality check program for all BAAs and performing periodic office/practice risk assessments can reveal vulnerabilities and unforeseen risks, which may affect your patients’ privacy and leave your practice open to possible breaches.

Once your homework is completed and data on vendors has been compiled, moving toward an all-electronic medical office can position you and your organization at the forefront of technology, security, and regulatory compliance.

Allan Ridings is a Senior Risk Management and Patient Safety Specialist at the Cooperative of American Physicians, Inc. (CAP).

For related information, see www.capphysicians.com.