Most people now have access to computers and mobile devices, and many use multiple devices including desktops, laptops, tablets and smartphones. All of this technology makes it much easier to communicate with others wherever one may be located. So it is not surprising that health care professionals, including psychologists, are using technology in their interactions with patients.

Psychologists can communicate with their patients in various ways using any of these devices. You can call, email, text or use instant messaging with your patient. There are also several free web-based applications for video phone conferencing that often are already installed on computers and mobile devices. Given the convenience, ready availability and ease of use, patients often ask to use these apps when they are unable to make their in-person appointments because they are traveling, ill or for other reasons.

But before psychologists launch into using Skype, FaceTime or instant messaging with their patients, there are a number of considerations to take into account. Many are outlined in the APA Guidelines for the Practice of Telepsychology (see article on page 6).

If you live in a jurisdiction where telehealth is governed by statute or regulation, it is imperative to review your state’s requirements for telehealth services to ensure your compliance. State laws vary considerably as to what technologies are included in the definition of telehealth. For example, while some states include email and telephone communications, many states specifically exclude email and phone from the definition of telehealth under laws mandating insurance coverage of telehealth services.

Informed consent

An overarching question to consider is how telepsychology fits within your practice. Consider your policies and procedures. In particular, review your informed consent agreement. Does it mention the possibility of providing services remotely, or is it geared toward in-person appointments and services?

As discussed more fully in the APA Telepsychology Guidelines, there are additional factors at play when providing services remotely compared to in-person settings. For those patients for whom telepsychology service delivery may be appropriate, your informed consent needs to address the potential benefits and risks of telepsychology.

Though the following list is not exhaustive, here are several issues to communicate in writing with your patient in advance as part of the informed consent process:

- Patient confidentiality – When communicating with your patient via Skype, phone or other modes, you are unable to ensure patient confidentiality to the same degree as when you meet with the patient in-person in your private, secure office. Does your patient understand
that patient confidentiality may be at risk when each of you is in a different location? Are you complying with the Health Insurance Portability and Accountability Act (HIPAA) in using these technologies for telepsychology services? For example, how is the electronic patient health information transmitted and stored?

• **Emergency situations** – You likely have protocols in place for handling emergency situations that may arise with patients in your office. Likewise, your outgoing phone message probably instructs callers to go to the nearest emergency room if they are having an emergency. But what do you do if your patient is in crisis during a telepsychology session? And what if your patient is either in another part of the state or even in another state? Have you discussed with your patient how to handle an emergency situation in such cases? Is there a designated emergency contact for your patient?

• **Technology failure** – You can count on technology failure. Your internet connection might drop or hardware may crash. You need to be prepared for the possibility of technology failure during a telepsychology session. Have you discussed with your patient in advance an alternate plan for either continuing the session or rescheduling the session should either of you experience technology problems?

• **Email or text messaging** – If you use email to communicate with patients, it is advisable for you to use secure email messaging when possible. You might also consider limiting use of email communications with your patients to administrative matters, such as scheduling or rescheduling appointments. If you choose to use email with your patients, you should also explain your policy for responding to emails to manage patient expectations and maintain boundaries. Further, if your patient asks to communicate with you via text, be aware that text messaging is not considered a secure means of communications.

• **Billing/reimbursement** – While a growing number of insurers appear to cover telehealth services, there is still variability among payers about whether telehealth is covered and if so, how such services ought to be billed. It is important to discuss this matter with your patient as he/she might assume that telehealth sessions will be covered similarly as in-person sessions. Your patient should review and understand his/her coverage. And if the session is not covered by insurance, it is advisable for the psychologist to clarify whether the patient wants to proceed with a telepsychology session or agree to pay out-of-pocket for the session. Also importantly, be aware that there may be “hidden” costs associated with telepsychology – for example, data plan overages and fees for service interruptions or technology failure.

**HIPAA/security issues**

While certain issues unique to telepsychology can be addressed in the patient informed consent, there are additional requirements that psychologists should consider. You need to assess how your use of telehealth affects your compliance with HIPAA requirements, particularly the Security Rule.

*Before psychologists launch into using Skype, FaceTime or instant messaging with their patients, there are a number of considerations to take into account.*

The HIPAA Security Rule protects electronic patient health information (ePHI) from unauthorized disclosure to or access by third parties. Therefore, psychologists who provide telepsychology services need to make sure that any ePHI generated during telepsychology services is protected. It is advisable to reexamine your policies and procedures for securing and maintaining ePHI to ensure that the information is appropriately protected.

The Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 modified obligations under HIPAA in several critical ways:

• Business associates are now directly liable under HIPAA for unauthorized disclosures of PHI that may result from performing certain functions on behalf of covered entities.

**MORE RESOURCES AT PRACTICE CENTRAL**

September 23, 2013, was the deadline for implementing changes required by the Health Insurance Portability and Accountability Act (HIPAA) Final Rule. To aid the process of compliance with the HIPAA Privacy and Security Rules, the APA Practice Organization (APAPO) has developed and updated several resources found in the HIPAA Compliance section of APAPO’s Practice Central website at www.apapracticecentral.org/business/hipaa/index.aspx.
Examples of business associates may include: third-party billing or practice management service; health care provider’s accounting firm or law firm that may have access to protected health information and transcriptionists or answering services. Not only is it important to have valid, signed business associate agreements with persons or entities who provide services such as claims processing, billing, utilization review or practice management; it is critical that those agreements reflect the business associate’s liability under HIPAA. Also be mindful that liability extends to any “subcontractors” of a business associate. However, you do not need a business associate agreement with other entities covered under HIPAA such as medical doctors, hospitals, clinics or insurance companies.

- In addition to paper files, patients are entitled to a copy of their ePHI in an electronic form and format requested by the patient. Generally, the covered entity must provide access within 30 days of the patient request.

- Breach notification requirements have changed. Originally, covered entities had to report any breach of PHI where there was a risk of harm to those whose data was disclosed without authorization. Now, covered entities must provide breach notification unless after conducting a documented, post-breach risk assessment, the covered entity can demonstrate that there was very little probability of PHI being compromised.

- Penalties for non-compliance with HIPAA requirements have increased. Civil penalties range from $100-$50,000 per HIPAA violation and maximum penalties for additional violations totaling up to $1,500,000. Criminal penalties include significant fines and/or imprisonment.

**Implications for practitioners**

So what does this mean for psychologists who would like to engage in telepsychology? Relevant considerations include the following:

- Is the technology or equipment you use HIPAA-compliant? This means that, consistent with the Security Rule, you should be able to control who can access certain equipment, software or data. You should have the ability to encrypt/decrypt ePHI when appropriate. (See sidebar on page 11 for a brief definition of encryption.) You ought to be able to monitor any unauthorized access or attempt to access electronic PHI. Any transmission of electronic PHI...
should be done through a secured network. For example, locking your wireless connection and setting a robust password for access will help protect your network from unauthorized access by strangers or unauthorized persons. By comparison, logging into a Wi-Fi hotspot at a coffee shop may not provide the same level of security or protection from unauthorized intrusions.

- If the vendor markets its product(s) as “HIPAA-compliant,” you need to do your homework and make sure that using that product fits within your existing policies and procedures for complying with HIPAA. Ask the vendor about authentication controls, audit controls, transmission security and breach notification functions. You may request a signed business associate agreement from the vendor acknowledging that the vendor is directly liable under HIPAA for any unauthorized breaches of patient health information.

- Be aware of the concern that many of the free, web-based telepsychology platforms do not comply with HIPAA. The platforms may not be able to provide an audit trail function to allow you to track who has access, to provide notification when an information breach occurs or to provide other capabilities including verified secure transmissions.

4 COMMON WAYS TO SECURE YOUR COMPUTER

Taking the following basic steps should help secure your electronic network:
1. Ensure that you are using antivirus protection.
2. Have robust passwords set for access to your Wi-Fi connection.
3. Have individual passwords for all family members or employees who may access your computers/system.
4. Set your computer, tablet or smartphone to automatically lock if it is idle for more than several minutes.

- With the increasing interest in telehealth technologies in health care, there are companies offering videoconferencing capabilities that claim to be HIPAA-compliant. Some even offer a business associate agreement. However, these companies charge a fee varying from monthly subscription to per session for videoconferencing services.