THE CARLAT REPORT PSYCHIATRY

A CME Publication

Subscribe today! Call 866-348-9279

AN UNBIASED MONTHLY COVERING ALL THINGS PSYCHIATRIC

Daniel Carlat, MD
Editor-in-Chief

Volume 13, Number 10
October 2015
www.thecarlatreport.com

IN THIS ISSUE

Focus of the Month:
Telepsychiatry

After reading these articles you should be able to:
1. Describe the role of telepsychiatry in today's psychiatric practice. **2.** Detail the types of privacy issues that practitioners need to be aware of when communicating with patients. **3.** List the types of confidentiality software available for practitioners.

Telepsychiatry: What You Need to Know

Daniel Carlat, MD
Editor-in-Chief, Publisher, The Carlat Psychiatry Report

Dr. Carlat has disclosed that he has no relevant financial or other interests in any commercial companies pertaining to this educational activity.

The Carlat Psychiatry Report last covered telepsychiatry back in 2010. At that point, it seemed like a cool technology that some of you might want to use. Since then, telemedicine in general has taken off, with an estimated 67% of physicians using or planning to use telehealth in

Continued on page 2

In Summary

- Recent studies have endorsed the efficacy of telepsychiatry.
- There are both free and subscription-based video teleconferencing services that can be categorized as "HIPAA compatible."
- As part of setting up a HIPAA-compatible telepsychiatry practice, you need to check with your state board and insurance carrier as well as discuss consent and privacy issues with your patients.

Q&A With the Expert

Integrating Technology in Your Practice

Jon Elhai, PhD

Professor of Psychology and Psychiatry University of Toledo

Dr. Elhai has disclosed that he has no relevant financial or other interests in any commercial companies pertaining to this educational activity.

TCPR: Dr. Elhai, you are a psychologist and researcher on PTSD, but I wanted to interview you because I know you have a strong interest in how mental health practitioners can use digital technology to communicate with patients. Before getting into some specifics or privacy protection, I'm curious about who is wanting to steal health information, and what they intend to do with it.

Dr. Elhai: There's a thriving black market for medical information. For example, people from other countries can use the information to create fake IDs to use healthcare services in the U.S. It can be used for Medicare fraud or to buy durable goods like wheelchairs that can be resold on the black market. Each individual's credentials can be quite valuable.

TCPR: Let's begin with something simple like email. HIPAA requires that any communication be encrypted, but what does that actually mean?

Dr. Elhai: When we talk about encryption in terms of the transmission of data, encryption is the mechanism that enables two people to talk to each other electronically only if they both have a special key—kind of like a password—that allows them

Continued on page 4

Telepsychiatry: What You Need to Know

Continued from page 1

their practices (https://www.americanwell.com/top-10-stats-you-need-to-know-about-telehealth/).

The appeal of telemedicine is clear, especially for psychiatrists. We are in great demand, and there aren't enough of us to meet the demand—especially in rural counties. Since our diagnosis and treatment usually don't require physical contact, we should be able to be quite effective via telepsychiatry. And patients are increasingly realizing that telehealth can save them the expense and time of schlepping to and from appointments.

A recent study quantified the amount of time and money our patients waste by having to show up to appointments. Using surveys from the Bureau of Labor Statistics, the researchers found that the average amount of time patients spend per visit was 121 minutes (37 minutes in travel time and 84 minutes in clinic time—including both waiting for the doctor and time spent there). Using average wage estimates, this equated to an "opportunity" cost of $43/visit (Ray KN et al, *Am J Manag Care* 2015;21(8):567–574).

So, the reasons to embrace telemedicine continue to mount, and luckily the technology has improved since our last article.

Does telepsychiatry work as well as face to face?

Before getting into the details of how to set up a telepsychiatry-capable practice, let's look at the crucial issue of whether telepsychiatry even works. We now have several studies endorsing its efficacy.

The most recent study randomly assigned 223 children with ADHD to 2 treatment groups. In the telepsychiatry group, children received 6 psychopharm visits by child psychiatrists delivered by videoconferencing. In the usual care control group, the children were treated in person by their PCPs who received telepsychiatry consultations. The kids in the telepsychiatry group did the best, significantly outperforming the PCP-treated group on all measures of ADHD (Myers K et al, *J Am Acad Child Adolesc Psychiatry* 2015;54(4):263–274).

Among adults, one study of depression randomly assigned 167 Hispanic patients to either webcam treatment (6 monthly video sessions) or treatment as usual at a community health center. Webcam patients were more satisfied with their treatment and had a more rapid decrease in depression severity than TAU patients (Chong J and Moreno F, *J E Health* 2012;18(4):297–304). Another study, which randomly assigned 126 women with PTSD to a trial of cognitive processing therapy either in person or via videoconferencing, found comparable outcomes in both groups (Morland LA et al, *Depress Anxiety* 2015 Aug 3 doi: 10.1002/da.22397).

Who pays?

Will insurance companies reimburse you for these visits? The answer is that it depends on the insurance. Medicaid is the most liberal, with 47 states allowing some reimbursement for telepsychiatry visits (see the website www.securetelehealth.com/index.php for great up-to-date information on various aspects of telepsychiatry, including insurance coverage). Medicare will reimburse for services if you are located in a designated underserved area of the country. In regard to private insurance, at least 30 states have passed laws requiring private insurers to reimburse telehealth to some extent. You'll have to contact your patient's insurance company to find out their policy.

A step-by-step guide

1. Decide on your technology. Here you have two major choices: free and debatably HIPAA compatible vs. not free and pretty clearly HIPAA compatible. The major free services are Skype, Google Hangouts, and Apple's FaceTime. In our article on HIPAA, we argue that the big three are "compatible enough" and that their convenience advantages outweigh the miniscule risks of a data breach. There are several other free or nearly free videoconferencing options now on the market that advertise themselves as being HIPAA compatible. We did some test runs of them (for more info, see our table, "Electronic Patient Communication: How to Keep It Private").

Some of you may want to be more cautious, in which case there are many pay options out there. While we didn't do a comprehensive survey, it appears that you can sign up for a HIPAA-compatible telepsych system for between $30–$300/month. This won't break the bank, and they may have some advantages over Skype et al. The video quality will probably be better. Depending on the price, there will be added features, such as virtual waiting rooms, mobile access, automatic patient billing, and e-prescribing. Some reputable companies include Cloudvisit Telemedicine (cloudvisittm.com), evisit (evisit.com), Secure Telehealth.com (securetelehealth.com), and Thera-link.com—listed in alphabetical order and with no implied endorsement.

By the way, if you were to do a Web search on telepsychiatry companies, as we did, you may become confused.

Continued on page 3

Telepsychiatry: What You Need to Know

Continued from page 2

Most of the websites listed in the search results are actually staffing companies that sell telepsychiatric services to institutions such as community clinics, nursing homes, or prisons. You have to dig deeper into the sites to figure out whether they actually offer services to private practitioners. There's a real Wild West feel to this industry, with many companies offering different services, making different HIPAA claims, and presenting bewildering pricing schemes that vary widely for offerings that are apparently equivalent.

2. Call your malpractice carrier. Most malpractice insurance policies will cover you for telepsychiatry, but you should check with your agent to be sure.

3. Check with your state medical board. In general, you must have a medical license in the state where your patient resides. A handful of states with dire shortages of physicians extend a special telemedicine license to out-of-state physicians. Some states require an initial in-person visit before you can practice telemedicine, but those are in the minority. Some state medical boards have very little to say about telemedicine. If that is the case in your area, you can follow the guidelines established by the Federation of State Medical Boards (https://www.fsmb.org/Media/Default/PDF/FSMB/Advocacy/FSMB_Telemedicine_Policy.pdf).

4. Inform your patients. Let your patients know that they have the option of seeing you via video visits, and have them read and sign a telepsychiatry consent form. Some examples of these types of forms can be found at www.azonlinepsychiatry.com/pdf/Telepsychinformconsent.pdf or www.communitypsychiatry.com/images/downloads/Telepsychiatry_Consent_Form.pdf.

5. Start seeing patients. Give your patients instructions on how to download whatever software you are using. Maintain professional standards as to your appearance (no pajamas!), and like any video encounter, be cognizant of what is in the background, noise level, etc.

For 2013 practice guidelines on video-based tele-mental health services, see www.americantelemed.org/docs/default-source/standards/practice-guidelines-for-video-based-online-mental-health-services.pdf?sfvrsn=6.

Electronic Patient Communication: How to Keep It Private

Communication type	Product	Cost	Description
Email	Virtual private networks (VPN) (Hot Spot Shield, Cloak, NordVPN, others)	Start at $3.00/month	Tunnels all your Internet traffic through an off-site private server
	Gmail	Free	Encrypted by default
	Virtru	$5.00/month	Works on top of any email provider to protect content, option for self-destructing email
Texting	Apple iMessage	Free	Encrypted only if both parties use an iPhone
	WhatsApp	Free	Both parties must download app
	Facebook Messenger	Free	May be linked to personal Facebook pages, security questionable
	Wickr, Wiper, Telegram, others	Free	Encrypted and option for self-destructing messages
Video	Skype	Free	Encrypted, software installation needed, HIPAA compatibility debated
	Facetime	Free	Encrypted, requires Apple operating system, software installation needed, HIPAA compatibility debated
	Google Hangouts	Free	Encrypted, cloud based (no software installation needed), multiple participants possible, HIPAA compatibility debated
	Vsee	HIPAA BAA only available with paid subscriptions; $299–$799/month plus set-up and training fees may apply	Encrypted, software installation needed, multiple participants possible, HIPAA compatible with paid version
	Doxy.me, Jitsi	Free	HIPAA compatible, no software installation needed, *TCPR*'s testing found both products relatively difficult to install/use
	Cloudvisit, evisit, Secure Telehealth, Thera-link, and many others	$30–$300/month	HIPAA-compatible video chat services usable with your patients, pricing varies according to added features
	HealthTap, Breakthrough, iCouch, Talkspace, and Talksession	Varying payment arrangements	HIPAA-compatible video chat services with a pool of patients looking to connect to doctors

Expert Interview
Continued from page 1

to send and receive communication. So if you're having an encrypted email exchange with a patient, for example, and someone tries to intercept that communication, the interceptor won't be able to read it unless they have the same special key as you and your patient (the sender and receiver). So even if that person was able to intercept the content of the communication, it is going to look like gibberish because they don't have a key to unlock that message, so to speak.

TCPR: Can someone intercept, or hack into, my communications at home even if I'm using my own router?

Dr. Elhai: Yes. If you're using a router that isn't set up with a password, anybody could just drive by and log onto your Wi-Fi. If someone is able to get on your network, it's pretty easy to intercept your electronic communications either by purchasing special software or doing a Google search on how to intercept email communication.

TCPR: So as long as I set a password on my home network, it's encrypted?

Dr. Elhai: Yes, but it's a little more complicated. There are two kinds of encryption types you can use. The less secure is called WEP (Wired Equivalent Privacy), and the more secure is called WPA (Wi-Fi Protected Access).

TCPR: And how do we select WPA over WEP?

Dr. Elhai: When you first use a new router, you will usually have the option of choosing different kinds of passwords, usually in a drop-down menu after you install the software. You simply select the WPA option, then create your password. WPA is harder to hack than WEP.

TCPR: So if both my patient and I have WPA passwords on our routers, then regular email using those routers is OK?

Dr. Elhai: Yes, as long as the passwords themselves are strong.

TCPR: What about if I'm using my computer at Starbucks? I assume those networks are very hackable.

Dr. Elhai: That's true if a password is not required. Public establishments don't always use encrypted routers because they want to make it easy for you to access their Wi-Fi. If you can hop on to the network of a coffee shop without a password, anybody with some technology skills could see what you're actually typing or what you're reading on your device. But often these days, there is a password, and if you use it, the encryption may be as good as you'd get with your home network. Of course, a café may be using the less secure WEP system. For example, if an establishment's Wi-Fi password is a pretty short numerical password, it may indicate a less secure WEP network.

TCPR: All right, let's say I'm in some public area, whether a café or a clinic, and I'm not very confident about the security of the network. Is there any way I can securely communicate with patients some other way?

Dr. Elhai: Yes. Some email providers have an "https" at the front of the Web address.

TCPR: In fact, I just logged onto my Gmail account in Google and it shows https in the address bar. What does that mean in terms of security?

Dr. Elhai: It means you are going through a secure socket layer-encrypted connection so that it is not possible to see what you're doing. Google now uses https as its default so that any Gmail communication is secure even if you're using a public Wi-Fi connection.

TCPR: That's reassuring. But let's say I'm using Gmail but my patient is using a provider that doesn't use "https". Can I assume our correspondence is protected because of my Gmail account?

Dr. Elhai: No, it's still hackable on their end. Keep in mind that encryption is only as strong as the weakest link. If you are receiving email from a server that doesn't use an https connection by default, then anybody who hacks into that connection could intercept your communication. So at a minimum, you'd want you and your patients to be using an email provider that encrypts by default.

TCPR: What other options are there to make sure email is private?

Dr. Elhai: Another way to go is to use a virtual private network, or VPN, which also provides protection if you're using a public Wi-Fi connection. The idea behind a VPN is that your Internet traffic is tunneled through your own VPN server off-site even if you're using a different wireless connection. That way, even if someone is able to hack into what you're doing or if you're using a site that is not https encrypted, no one would be able to see it because all of your Internet traffic would be securely transmitted to a non-local, private server.

TCPR: This sounds ideal for doctor-patient communication. But aren't VPN servers really expensive?

Dr. Elhai: They used to be, but not any longer. You can now subscribe to a VPN service for an average cost of $5.00 per month. Some of the more popular VPN providers are HotSpotShield, VPN Unlimited, Cloak, and Hide My Ass. Once you are connected, they are pretty simple to use; you just go into their app and click a button to connect to the VPN.

TCPR: So if a patient is using the same security email provider that I'm using, or if I'm using a VPN, I can feel pretty confident about the security of my emails. Still, we are sometimes talking about very sensitive clinical information. Are there any further levels of security I should be thinking about?

Dr. Elhai: There is also another type of technology called Virtru that I sometimes use when I send sensitive information. Instead

Continued on page 5

Expert Interview

Continued from page 4

of using standard encrypted Gmail, Virtru sends an email from my Gmail account to the recipient saying something like, "You have an email encrypted through Virtru. Click here and you will be taken to a Virtru server to see that email." Virtru also lets you do things like disable forwarding of an email message or set a time limit to delete messages from the server after a set number of days. Using Virtru is basically like wrapping your email client with self-destructing encryption.

TCPR: There is an ongoing debate about how HIPAA compliant Skype, FaceTime, and Google Hangouts are (see the article in this issue that addresses this topic, "Are Skype, FaceTime, and Google Hangouts HIPAA Compliant?"). Are there any solutions that make video teleconferencing a more secure option—without costing an arm and a leg?

Dr. Elhai: Yes. One of the solutions is a free service called Jitsi that adds an additional layer of protection from interception. There is also something called Doxy.me, which is also free as well as HIPAA compliant. AK Summit is another one. I don't think you need to spend thousands of dollars to buy special hardware services from telecommunication companies that provide high-end telemedicine solutions given these free security and privacy solutions.

TCPR: So if I download a solution like Jitsi or Doxy.me, would my patient have to download it as well, or is it secure if I have it just on my end?

Dr. Elhai: Ideally you'd want both the sender and the receiver to use it to ensure that extra layer of protection. The Electronic Frontier Foundation (www.eff.org), which is a nonprofit organization that advocates for digital Internet rights, has evaluated a lot of the videoconferencing services out there. With Skype, you can do video as well as audio calls and instant messaging. Google Hangouts is basically an alternative to Skype. One advantage of Google Hangouts is that it lets you communicate with multiple people at the same time for free. With Skype, you pay an added fee for a multiple-video connection. And then there's also the platform. Apple tends to be one of the companies that focuses on privacy and security a little bit more than some of the other ones, so FaceTime has that to offer. You cannot currently use FaceTime across different phone or computer platforms. Unlike FaceTime, however, you can use Skype and Google Hangouts on either an Apple or an Android device. You probably want to use a platform that is universal enough so that you can communicate with your patients no matter what type of device they are using.

> **"Encryption is only as strong as the weakest link. If you are receiving email from a server that doesn't use an https connection by default, then anybody who hacks into that connection could intercept your communication."**
>
> Jon Elhai, PhD

TCPR: Finally, what about text messaging? Is that a secure way to communicate electronically?

Dr. Elhai: It depends on the type of messaging. Many people use iMessaging on iPhones, and as long as both the sender and receiver have an Apple device, these messages are extremely secure. Not only are they encrypted, but they are encrypted in such a way that even Apple can't read the message. However, I would not use standard SMS text messaging with patients, which is not encrypted.

TCPR: What's the difference between an iMessage and an SMS message?

Dr. Elhai: Say you are using an iPhone to send a text message. The message will look blue if you are sending it to someone who has an Apple device because it's being transmitted through iMessage, which is Apple's own closed system. But if you're sending a message to someone who doesn't have an Apple device, the messages appear green, which means it is being transmitted as a standard SMS message. SMS messages are not encrypted.

TCPR: What options are there for sending encrypted text messages using non-Apple platforms?

Dr. Elhai: There are other closed platforms for messaging. You could send a message through Facebook—that would be closed, but it's not necessarily private. The most popular messaging platform is currently WhatsApp, which is very secure, but it requires both the sender and the receiver to have a WhatsApp account. Whereas with standard messaging, as long as you have someone's number, you can text message them without using a specific platform. That's a convenience vs. security issue. There's also a newer wave of messaging apps that provide both encryption and self-destructing messaging. Some of these are called Wickr, Wiper, and Telegram.

TCPR: What would be the easiest way for us to discuss with patients how to message each other?

Dr. Elhai: Your best bet with patients is to establish under what circumstances you want to be text messaging with one another. Usually it's for something brief like confirming or canceling an appointment. If you both have iPhones that makes it easy. Otherwise, choose a secure platform such as WhatsApp, or one of the other popular services like Wickr, rather than standard messaging. You also want to confirm that your patients have passcodes on their phones and discuss any privacy risks if their phones were stolen and/or someone read their messages. By the way, I'm talking about fairly strong passwords, not just like 1111 or 1234. Using a digital fingerprint is also a good way to ensure security if your phone is lost or stolen.

TCPR: On a final note, what are the legal ramifications to our technology use? I haven't heard of a lot of doctors getting sued for trying to communicate with their patients and taking reasonable precautions, but is this something we need to

Continued on page 8

Are Skype, FaceTime, and Google Hangouts HIPAA Compliant?

Daniel Carlat, MD
Editor-in-Chief, Publisher, The Carlat Psychiatry Report

Dr. Carlat has disclosed that he has no relevant financial or other interests in any commercial companies pertaining to this educational activity.

It's been quite a while since we discussed HIPAA (see *TCPR*, July 2005 for our interview with Rebecca Brendel). So let's do a quick review.

As you undoubtedly know, one of the purposes of HIPAA, a law originally passed in 1996, is to regulate the flow of protected health information (PHI). It says that you are allowed to communicate PHI in certain circumstances—like to collaborate with other doctors or to get paid by insurance companies. But it also lays out a series of safeguards that you have to take to make sure nobody outside this circle of knowing gets their hands on PHI. For example, you have to make sure you or your staff don't talk about patients in public, you shouldn't leave charts out where people can see them, and if you use an electronic health record (EHR), you have to make sure that it has a good protocol to prevent data breaches.

Applying HIPAA to telemedicine has proven to be pretty tricky. A decade ago, most of us believed that the only way to ensure secure videoconferencing was to pay for expensive "HIPAA-compliant" videoconferencing equipment. This severely limited telemedicine's economic feasibility. But things are changing. There are many more free or nearly free videoconferencing platforms, and most patients and doctors are quite comfortable using them.

Unfortunately, there is no agreement on whether all the free platforms are HIPAA compliant. One source of confusion is the misconception that a specific technology can even be "HIPAA compliant." In fact, the only entities that can be HIPAA compliant are providers themselves. The federal government requires only that we take "reasonable administrative, technical, and physical safeguards" to ensure the confidentiality of patient information. Furthermore, the HIPAA Privacy Rule is "flexible and does not prescribe any specific practices or actions that must be taken by covered entities" (see https://www.healthit.gov/sites/default/files/nationwide-ps-framework-5.pdf)

This means that you have to use your own judgment regarding what technologies are private enough, based on guidance provided in the HIPAA law. Instead of "HIPAA compliant," the better term for evaluating these systems would be "HIPAA compatibility," and there is a spectrum here. Systems can be more HIPAA compatible, or less.

There are three HIPAA guidelines that relate to telemedicine:

1. Encryption. All communication between you and your patient should be protected, and the best way to achieve this is to encrypt such information. Encryption ensures that if anybody hacks into your conversation, all they will see is gobbledygook—unless they have the encryption key. Skype, FaceTime, and Google Hangouts all encrypt their data, probably at a level that is stringent enough to meet HIPAA guidelines.

2. Business Associate Agreement (BAA). HIPAA defines a "business associate" as any company that: a) helps you run your practice, and b) has access to PHI. Business associates include your billing company, your answering service, your transcriptionist, your EHR vendor, and others. All these services require either storage of PHI or entrusting people to see the information. HIPAA requires that all of these specially defined business associate sign a contract stating that they will keep your patients' health information secret. This is the so-called business associates agreement, or BAA.

Skype, FaceTime, and Google Hangouts do not offer such agreements (though Skype offers a paid business version that does). So they're not HIPAA compatible, right? Probably wrong—because of a HIPAA provision called the "mere conduit" exception. If a company is not in the business of actually storing PHI, but simply helps to transmit it from point A to point B, then it doesn't have to sign a HIPAA business agreement. The analogy often used is a mail courier service, like FedEx. FedEx transports packages from place to place, but the company does not open them. Similarly, Skype transmits encrypted information but does not look at it or store it anywhere for review.

Not everyone agrees that Skype qualifies as a "mere conduit." A common argument is that since Skype cooperates with law enforcement to investigate criminal communication, this means that the company does have a digital "back door" that could potentially be hacked by the bad guys (though this has not happened). Because of this admittedly remote possibility, some people contend that Skype should be treated like a business associate.

We don't agree with that argument, but we acknowledge that it is a debatable point. For us, the fact that Skype (and FaceTime and Google Hangouts) securely encrypt all transmissions makes these technologies sufficiently HIPAA compatible.

As a bit of an aside, given the gnashing of teeth about Skype's privacy, why don't we ever hear worries about the simple telephone? Surely the phone, the constant victim of wiretaps in crime dramas, can't be HIPAA compatible? Most experts seem to avoid this question—but some say that tapping a phone is actually much harder than hacking into email. That's good enough for me!

3. Monitoring for breaches. You're supposed to have a way of monitoring any communication you use for breaches, and the government should be able to audit it. Skype won't provide you with a report like this. On the other hand, there have been no reports of hackers actually listening in on conversations—the main risk is that hackers could look at your call log.

The bottom line is that Skype,

Continued on page 7

CME Post-Test

This CME post-test is intended for participants seeking AMA PRA Category 1 Credit™. For those seeking ABPN self-assessment (MOC) credit, a 13 question pre- and post-test must be taken online. For all others, to earn CME or CE credit, you must read the articles and log on to www.TheCarlatReport.com to take the post-test. You must answer at least four questions correctly to earn credit. You will be given two attempts to pass the test. Tests must be taken by October 31, 2016. As a subscriber to *TCPR,* you already have a username and password to log on www.TheCarlatReport.com. To obtain your username and password or if you cannot take the test online, please email info@thecarlatreport.com or call 978-499-0583.

The Carlat CME Institute is accredited by the Accreditation Council for Continuing Medical Education to provide continuing medical education for physicians. Carlat CME Institute is also approved by the American Psychological Association to sponsor continuing education for psychologists. Carlat CME Institute maintains responsibility for this program and its content. Carlat CME Institute designates this enduring material educational activity for a maximum of one (1) *AMA PRA Category 1 Credit*™ or 1 CE for psychologists. Physicians or psychologists should claim credit commensurate only with the extent of their participation in the activity.

Below are the questions for this month's CME post-test. This page is intended as a study guide. Please complete the test online at www.TheCarlatReport.com. Note: Learning objectives are listed on page 1.

1. The mechanism that enables two people to talk to each other electronically only if they both have a special key that allows them to send and receive communication is called: (Learning Objective #2)
   - [ ] a. Non-repudiation
   - [ ] b. Encryption
   - [ ] c. A router
   - [ ] d. Geoblocking

2. What is one advantage of using Google Hangouts for videoconferencing as opposed to Skype or FaceTime? (LO #1)
   - [ ] a. It lets you communicate with multiple people at the same time free of charge
   - [ ] b. It blocks standard SMS messaging with patients
   - [ ] c. Your Internet traffic is tunneled through your own VPN server off-site
   - [ ] d. It offers end-to-end encryption so that law enforcement can require access under privacy restriction rules

3. Which of the following is not a HIPAA guideline that relates to telemedicine? (LO #2)
   - [ ] a. Business associate agreement
   - [ ] b. Monitoring for breaches
   - [ ] c. Compliance
   - [ ] d. Encryption

4. Approximately what percentage of physicians use or are planning to use telehealth in their practices? (LO #1)
   - [ ] a. 35%
   - [ ] b. 67%
   - [ ] c. 82%
   - [ ] d. 98%

5. HotSpotShield, Cloak, and Hide My Ass are examples of which type of internet privacy tool? (LO #3)
   - [ ] a. Virtual Private Network (VPN)
   - [ ] b. Wi-Fi Protected Access (WPA)
   - [ ] c. Wired Equivalent Privacy (WEP)
   - [ ] d. Encrypted Video Platform (EVP)

PLEASE NOTE: WE CAN AWARD CME CREDIT ONLY TO PAID SUBSCRIBERS

Are Skype, FaceTime, and Google Hangouts HIPAA Compliant?

Continued from page 6

FaceTime, and Google Hangouts are all encrypted video platforms that are widely adopted, easy to use, and free. Their official HIPAA compatibility is the subject of ongoing debate, but many clinicians use them anyway.

For an excellent in-depth discussion of Skype's HIPAA issues, see the free Web article: www.zurinstitute.com/skype_telehealth.html.

For a good overview of HIPAA in general for psychiatrists, see the APA website: www.psychiatry.org/psychiatrists/practice/practice-management/hipaa (available to APA members only).

❖ ❖ ❖

THE CARLAT REPORT: PSYCHIATRY

P.O. Box 626
Newburyport, MA 01950

PRSRT STD
US Postage
PAID
Nashville, TN
Permit 989

This Month's Focus:
Telepsychiatry

Next month in *The Carlat Psychiatry Report:* Psychiatry and General Medicine

Expert Interview
Continued from page 5

be wary of down the road?

Dr. Elhai: I haven't seen any examples of legal action at the individual doctor level, but certainly there have been recent class-action lawsuits filed against companies who have been hacked, and several hospital systems have also been hacked as well. So I suspect lawsuits would probably target the organization first, but doctors are part of organizations, and if there is a particular doctor who is being especially negligent with patient communication in a non-secure way, that could be a problem. So, yes, I think electronic security should be a concern for clinicians, especially more so in the future as hacking gets more widespread and sophisticated.

TCPR: Thank you for your time, Dr. Elhai.

❖ ❖ ❖