Defense Centers of Excellence for Psychological Health and Traumatic Brain Injury (DCoE) Webinar Series

March 26, 2015, 1-2:30 p.m. (ET)

"Legal, Ethical, Security and Privacy Issues Relating to the Use of Behavioral Health Technology Tools in Clinical Care"

Good afternoon. Our moderator today is Dr. Kathleen Charters. Dr. Charters is a Certified Professional in Healthcare Information Management. She spent 25 years as a learned expert in informatics with the United States Navy. She is currently a Nurse Consultant for the Defense Health Agency at their Healthcare Operations Directorate and Clinical Support Division. Her current area of focus is on creating infrastructure to support enterprise quality assurance, patient safety, and risk management. Dr. Charters participates in transition planning for moving from legacy to modern electronic health records, including eMeasures, Blue Button and Patient Portal.

Welcome, Dr. Charter.

Thank you, Dr. O'Donnell, for that wonderful introduction.

Good afternoon and thank you for joining us today for the Defense Centers of Excellence Psychological Health March webinar. Before we begin, let us review some webinar details. Live closed captioning is available through Federal Relay Conference Captioning. Please see the pod beneath the presentation slide. Should you experience technical difficulties, please visit www.dcoe.mil/webinars and click on the Troubleshooting Link under the Monthly Webinars heading.

There may be an audio delay as we advance the sides in this presentation. Please be patient as the connection catches up with the speaker's comments.

Today's presentation and resource list are available for download in the Files pod. If you preregistered for this webinar and want to obtain a CE Certificate or a Certificate of Attendance, you must complete the online CE posttest and evaluation. After the webinar, please visit www.continuingeducation.dcri.duke.edu to complete the online CE posttest and evaluation and download your CE Certificate or Certificate of Attendance. The Duke Medicine website online CE posttest and evaluation will be open through Thursday, April 2, 2015, until 11:59 p.m. Eastern Time.

Throughout the webinar, you are welcome to submit technical or content-related questions via the Q&A pod located on the screen. All questions will be anonymous. Please do not submit technical or content-related questions via the Chat pod. Participants are encouraged to chat amongst each other during the webinar, using the Chat pod; but please refrain from marketing or promoting your organization or product in the Chat pod.

I will now move on to today's webinar topic. As behavioral health care providers embrace the integration and incorporation of technology into current practice, it is important to understand both the benefits and risks. This presentation will include a discussion of statutory and regulatory guidance regarding security and privacy issues involving telehealth and other types of behavioral health technology tools in the clinical

environment. Specifically, it will address the Health Insurance Portability Act of 1996 or HIPAA; the Privacy Act and related DoD guidance; and will discuss ethical considerations regarding the use of technology in a clinical setting

During this webinar, participants will learn to: identify security and privacy risks related to the use of mobile technology in clinical care; evaluate potential security and privacy risks in current clinical practice; implement administrative, physical and technical safeguards used to protect patient data; and Interpret the security and privacy guidelines and be able to explain them to patients to allow them to make informed decisions regarding their health data

I would now like to introduce our presenter, Mr. Bryan Wheeler. Bryan Wheeler serves as Deputy General Counsel of the Defense Health Agency in Falls Church, Virginia. Previously, he served as an Associate General Counsel with the Office of General Counsel, TRICARE Management Activity in Falls Church, Virginia, with primary duties as counsel to the Defense Centers of Excellence of Psychological Health and Traumatic Brain Injury and the TRICARE Regional Office-North.

He completed a BA in Political Science at the University of the State of New York while on active duty in Washington in October 1983 and subsequently graduated from Washington University School of Law in 1987 with his Juris Doctorate. He is a member of the State Bar of Kansas and is licensed to practice before the United States Supreme Court, the Court of Appeals for the Armed Forces, Supreme Court of Kansas, and various federal, district and appellate court.

After retiring from the Air Force and prior to assuming his current duties, he served as the Deputy Director, Investigative Project on Terrorism, a counter-terrorism think tank in Washington D.C. He has appeared on CBS 60 Minutes and National Public Radio's All Things Considered. In 2013, he also co-authored the article, Fighting Health Care Fraud in Bold and Innovative Ways in the ANFIS Journal.

Thank you and welcome, Dr. Wheeler.

Thank you.

It's good to be here this afternoon. We've got a topic before us in this period that could take all of a graduate-level semester, and all we have here this afternoon are what – three hours? A little bit of humor there for all of you but very little. This can be a complex area, and we're going to be touching on highlights and things that you need to be concerned with as a practitioner. But keep in mind that this is an area of the law that continues to evolve.

With that, today we're going to be talking about telemedicine licensure, credentialing and privileging issues and reimbursement. But it's going to be much more than that as we look at how the law, how regulations, and how privacy concerns and ethics affect what we do.

Next.

That's a disclosure. Once again, I'm speaking for myself and not the Department of Defense, the DCoE, or the Defense Health Agency.

Next.

Now, first of all, when we talk about some of the legal considerations, we're going to discuss a little bit of the history of the law in this area, how it's changed; we're going to touch on some of the security and privacy issues that you need to be concerned with as practitioners; and then we're going to talk about some practical and ethical concerns that you may have when you practice; and also we'll touch on some cultural considerations.

Next.

Doesn't this pretty much sum up for you what the law is: "Yes, I suppose instigating fights between people then stealing their food during the chaos could be considered a survival skill…and thus began the legal profession."

So when we look at the law on this, it has changed. And telemedicine is predominantly concerned – the area of the law that we are concerned with is privacy. So if you went back and did a survey of the law on privacy, pretty much in the United States we trace our lineage on that from Great Britain; and you go back to the Magna Carta, and not a whole lot changed for centuries. And in this country, there was a very slow evolution, finally culminating with some important recognition in the 1960s in a series of cases that very much affect health care, such as Griswold v. Connecticut.

Even though we had these Supreme Court cases going on, there was recognition by many that we needed to do more than just let the common law continue to affect things. And so Congress passed the Privacy Act back in 1974. We're all familiar with it. Any dealings with the Federal Government, we continually have to sign a release with pretty much every interaction we have, whether it's with the IRS or with our employment or what have you.

And generally, all we're concerned about there is just advising people that we do have privacy, and we respect your privacy; but if you want to get certain work conducted with the Federal Government, you're going to have at least give some of that privacy up so we can consider it. And things stayed fairly docile, I guess, in the medical area with protections largely being done at the state level. And so there was recognition that there are many inconsistencies between states.

And the Federal Government decided in 1996, there was an Act in Congress, the Health Insurance Portability and Accountability Act. Part of that Act included a provision of law that any of the practitioners here I'm sure are quite familiar with and require it at annual training, and we refer to that as HIPAA. But in particular, we get concerned with the HIPAA privacy rule and how that affects us. And I'm not going to give you your HIPAA training right now, but I use it to illustrate how the law has continued to change.

Now, the HIPAA rules apply with anything that you're going to be doing if you're working as a Federal practitioner. Whether it's DoD, VA, or HHS, that will be the default position. If you're in a jurisdiction that has a more restricted rule that provides (inaudible), say California for example, and you're practicing outside of the scope of the Federal Government, then you're going to need to get very familiar with that jurisdiction's law on privacy; and you'll have to comply with it.

If you work for the Department of Defense or the Department of Veterans Affairs or HHS, not a problem; they'll follow HIPAA within our Federal practice. There could be some issues where things overlap; and if we get to those difficult cases, we can provide an interpretation on it. But in general, the default position will be we will follow the Federal Rule and involve HIPAA.

I cite there the HITECH Act of 2011 just to illustrate that with our technology and all the things that it's bringing forth, there are new risks that also come into play. And with the HITECH Act, there is a recognition that the current rules weren't explicit enough for how we deal with the breaches of data. Ordinarily, I would think in what we would be doing with telemedicine, we probably won't have to worry about the HITECH Act unless, of course, we have a disaster and then there would be reporting requirements that your agency will have to make.

Next.

If you work within DoD and you do telemedicine, you're probably familiar with this memo that Dr. Woodson – he's the Assistant Secretary of Defense for Health Affairs – this memo that he issued in December of 2012. And one of the things that he referenced in that and his reason for doing that was to implement what is called the STEP Act, which is one of the changes to the National Defense Authorization Act -- I believe it's 2012 -- that gave us Naval authority for how we deal with telehealth.

And so one of the great things about it, if you're a practitioner outside of telehealth and you work for the Department of Defense – say you're a uniform provider or a civilian GS provider or a pension services contractor working in one of our facilities – you have portability of licensure. What that means is today we're taking this presentation and doing it in Virginia. So if you're licensed in Virginia and you get reassigned through work to Maryland – say you work at Fort Belvoir and you get reassigned to work over at Walter Reed over on the Maryland side – it's not a problem because you've got portability of licensure.

If Dr. Woodson or your Surgeon General or whomever decides that you need to go out and work in Washington State or California, it's not a problem. You're licensed in a jurisdiction, so you have portability of licensure and you won't have a problem as you might if you worked outside of the government.

Well, when we get to telemedicine, things aren't necessarily so clear. And so what happened after this memo was released is that -- I believe it was the next slide – okay, this is wrong – if you want your own copy, you can find it on the Health Affairs website. But probably more importantly, I would advise you to look at the Department of Defense Manual 6015.23. And this manual was updated in October of 2013. And one of the things that the manual does, more so than just Dr. Woodson's memo, is that it provides how we go about credentialing providers within DoD who provide telemedicine services.

So I was just talking with Dr. O'Donnell before we started here today about some of the Medicare rules and the terms that they use. And the good thing about it is that our rules are very similar to Medicare's rules in that we use some of the same technology, such as the distance site and the originating site. What we provide for here is that if you're licensed within the DoD system, you will be allowed to do your work at an MTF or wherever -- we're going to call wherever the provider is, that's the originating sight; where the patient is located is going to be the distance site.

Currently within the Department of Defense, you will be working at an MTF if you're providing telemedicine services or at a DA facility. 6025.13 does provide that you could have a VA practitioner providing the telehealth services. In discussing with Dr. O'Donnell the state of things, as I note, that's what the current rule is. Of course they're looking at other options because there are some providers who would like to be able to, perhaps, treat a patient using telemedicine in a patient's home versus at an MTF. Currently, we don't do that within the Department of Defense.

We may, at some point in the future, decide that is what we want to do. And if we do that, obviously, you'll be finding maybe that the safety net for proceeding with the treatment is going to work and obviously there will be some criteria about when it's used. But if you have questions about how did we go about doing telemedicine credentialing, I invite you to go ahead and look at the DoD Manual, 6025.13. And that's available on the DoD website; or if you just Google it, it will come right up.

I also wanted to point out – I didn't mention it earlier – but if you have questions, please feel free to go ahead and submit them; and we'll have a chance to discuss them as we go along.

The next slide there is the PC Coach, actually the PE Coach, the DCoE platform. And I hope that we've got some providers out there that are familiar with the PE Coach. One of the things that I noted earlier, why it's more than just telemedicine, is that this is an example of a technology that is not simply the typical way that we think of telemedicine with a provider being in one location and rendering medical services across a distance using technology, typically (inaudible) technology.

Instead, this is something you can use with your Android or your IOS device; and it's used for treatment of patients with PTSD for prolonged exposure.

Next slide, please.

I've got an example here to discuss. Let's say you're a provider and you're using the Prolonged Exposure, PE Coach, with one of your PE patients. In this instance, you go ahead and you've saved an audio recording; and it's backed up by another audio app that the person has on their phone – their

iPhone or Android device – and it's uploaded to the cloud. And then the recording is accessed by a friend who has access to their audio uploads.

Doctors, what are the clinical app implications of this? Does anyone want to tackle that one?

[Pause for responses]

Well, so we'll go ahead and work through that. One of the things – and we're going to talk about in a bit for addressing this proactively – but hopefully you will advise the plan of the patient what the implications were of the app – of what is it doing. And so the application is one where you store information. Any time you store information, there is a risk. The risk could be that if it's a diary or a journal, that somebody can come across that, and you want to safeguard the information. With technology, it gets obviously a little trickier because once information is uploaded to your cloud, there's always the risk that a third party can come across it.

In this case, this is the person's friend. So from a clinical standpoint, the best way of dealing with this of course is to discuss with the patient beforehand the risk in the practice that if they use this what they intend to do.

Are there any questions?

All right, let's go to the next slide.

All right, T2 Mood Tracker – if we were in a large lecture hall, I'd ask you to raise your hands; but we don't have that luxury. But I'd be curious to know how many people out there have uploaded it. It's a very popular app that T2 has developed.

Next slide, please.

We'll get to the case discussion here. So let's say you've decided to use Mood Tracker with one of your patients or clients. This person is bipolar. And they would like to send you, their provider, a screenshot twice a week of where they're at using Mood Tracker. In case you're not familiar with Mood Tracker, just note it is an application that allows an individual to note where they're at as far as how they're relating to their environment and stresses in their life. And there's a scale there that the patient can use, the client can use; and it shares information with the provider.

Many providers would choose to just have the patient bring it in, much as they would a journal or a workbook or some sort of assignment that they could go through with the patient or client. In this instance, the patient wants to send the materials in by a screenshot. And then you'd have the capability in this scenario of putting it into the patient's electronic health record. What security/privacy concerns would you have here?

Well, again, it's going to be very similar to the issue that I noted earlier using the prolonged exposure app. In the meantime, you've got information recorded. There is the issue of a breach. So somebody else could review the material so that the patient/client could be embarrassed by it.

There is also a concern, of course – and we'll touch on it here in a bit – that the network might not be secure. So I've got an iPad here, right? If I wanted to use this iPad someplace, typically I'll get a warning that will pop up that will tell me whether or not it's secure. If it's not secure, then certainly there's that risk. And one thing you want to make sure when you use your iPad is to know what it's doing when you're talking.

So here at home, my iPad is actually transmitting some news that I was unaware of if I didn't have that app on there. Anyway, the risk is that information could be disclosed; and so you need to caution the patient when you use this that there is that risk. And that's probably the predominant concern you have.

Now let's talk about security concerns. You've got the person using the Mood Tracker; and the person says, "I'm highly stressed. I need to talk to someone. I need to talk to someone right now." And the person communicates this screenshot, presumably probably by e-mail. What's one of the problems with e-mail? It's really great; it's asynchronous. But because it's asynchronous, that may well mean that there's not a person at the other end that's receiving it. And so if you're a provider and you're wanting to utilize this technology, you need to advise the patient or client what the limitations are. And that if you're going to be transmitting something electronically, it means that there may not be somebody at the other end when that happens.

We've got another case example. Let's go to the next one here.

So there's Fitbit, and there are many other handheld or wrist-type devices out there that are very popular right now. And let's say you've got a patient who is wearing one of these; and they're using it to track their exercise, their caloric intake, their sleep. They also use the Mood Tracker that we just talked about. And they transmit all this information to your personal phone, as well as they're using their personal phone, not a government BlackBerry or iPhone or something.

What type of security or privacy concerns would you have or would you want to consider?

[Pause for responses]

Well, once again, as always, there is the risk that it can be disclosed. I'll tell you within our Federal practice, specifically within the Department of Defense, we caution against transmitting information to your provider using some sort of unsecure means. Mainly we're concerned about breach is the big thing because if it's unprotected, there's no telling who would get the information. Obviously, if you look at all the things that are going on in our world with technology, many of us have had financial information taken from us, maybe somebody getting access to your credit card or something like that.

Well, with health information, it can be extremely embarrassing, particularly in the area here that we're tending to deal with at DCoE, which is psychological health. There may be information there that could be embarrassing to someone. It could affect their work – more than just affect their work, whether or not they have any work, whether they go on in their field – as well as any number of other concerns. So that's a huge thing that needs to be discussed with the patient or client before using this technology in transmitting information.

I see some of the comments here. The phone could be stolen. There's a case before the Supreme Court right now involving the question of what is secure on a telephone. It used to be, before we had handheld phones, that everything you could do with phones we've done with the landline. And so there were limits to how those calls could be intercepted; and you needed to have a search warrant, for example if it's law enforcement wanting to record someone's phone. You had to get a magistrate, you had to get a judge, and get permission to do it.

Well, with handheld devices, these days it's more than just a simple communications devices; it's their entire computer. And for some people, that can have almost their entire life in it. They've got all their financial information; they've got a lot of personal information with their significant other and friends and family and what have you; they have photographs. And now, within this setting, we're talking about yet in another direction with their health information; and so with that, there is always the risk that this information could be stolen.

One of the things that we do with our government devices is that we've got a requirement that, with BlackBerry for example and our government laptops, they've got a software program within them that essentially protects data at rest, meaning if someone steals your laptop, if it has the correct software on it, then that information is going to be protected. But if it's your personal phone, chances are you haven't invested in that software; and it's not protected. So if someone steals it, that information is going to be compromised.

Any questions along those lines?

[Pause for responses]

Let's talk about the Guidelines for the Practice of Telepsychology. You can read that: "The provision of psychological services utilizing telecommunication technologies; psychologist's proper knowledge of and competence in the use of telecommunication technologies; and the psychologist's need to ensure that client/patient has a complete understanding of the increased risks to loss of security and confidentiality when using these telecommunication technologies; and an understanding of interjurisdictional practice. So there's a whole lot that we could talk about here. We could devote several hours of discussion to that. We're not going to do that.

Next.

We have three standards listed there from the APA as far as how they apply here: competence, human relations, and confidentiality.

So what are some of the issues – I'll open it up – any questions that people have as this interacts with their practice for ethics they're concerned about?

[Pause for responses]

None? All right, well, the American Psychological Association has a task force on telepsychology that was created in 2012. And they looked at these unique characteristics that technology brings to the provision of clinical care. And they're distinct from those that we typically see in a normal, non-telemedicine setting. And they've developed these guidelines that we just discussed.

Next slide.

Let's talk about this. If you're using a treatment or tool in therapy that you're not familiar with, what items would you want to consider? Let's take psychology. Anyone – what ethics codes might inform you on how you'd answer the question?

Let's look at Rule 2.01, Boundaries of Competence. Psychologists who are planning to provide services, teach or conduct research involving populations, areas, techniques, technology newness, need to undertake education and training (inaudible) complication of study before doing it. We need to know what it is we're doing and get a good lay of the land on this.

And if you have questions, then you talk to your colleagues, talk to a legal professional if you've got questions on the law, certainly about risk; and I'd advise you to read up on it. There's a lot of material on it. You can go to the APA, for example, they've got materials on their website that can help you get educated on that.

One of the things that we talk about with these technologies is that a lot of times when a technology is created, we don't know all the risks. And sometimes we can't even fathom the risks that are there. So I started to discuss a couple minutes the idea of privacy in a cellphone; and by the cellphone, I mean the smartphone and the quality items that are on there. We're still figuring out what the law is on that and the extent of it.

So you have the local jurisdiction here in the Washington D.C. area who has decided that if they arrest an individual, they can seize that phone; and they can go through all of the contents on it. It's like seizing their computer to many people, but instead they look at it (inaudible), which is a lot like their telephone. So the example we've got there is you have somebody back in the days when you had a beepers, you could look and see where the phone call was coming from and you could look at that. But now the Supreme Court is going to be coming down with a decision in June, most likely, on just what information is legally protected on one of those phones.

And it's going to be interesting to see how that affects medical practice, and the way that it would probably most likely come across would be in the area of informed consent that we would provide for somebody if they're using an application on that phone. It's an area of the law that is in flux, and we'll see more guidance coming out this year on it.

Now, I note that as these new technologies come along, there are standards for training that still need to be worked on. And so even though when a new technology is created and people are quick to be first adopters, sometimes you don't have all the training that you need for those things. It's just part of the nature of the evolution of training. So in any event, when you're using a new technology, a psychologist needs to take reasonable steps to ensure the competence in their work and protect the clients' and patients' information, as well as if they're in a teaching environment, students, to provide these research participants or organization clients.

So there we go. We have Calvin and Hobbes here. Calvin said, "I read the ethics book you got me."

Mom says, "What did you think of it?"

He says, "It really made me see things differently. It's given me a lot to think about.

She says, "I'm glad you enjoyed it."

He says, "It's complicating my life. Don't get me any more."

As we see new technology, there are things that come about that maybe we never anticipated. Sometimes it's like we were recreating the wheel again when we look at new devices and how it could affect people, particularly when we're talking about transmitting information that is as sensitive as what we have here.

Next.

We're going to discuss competence, the boundaries of competence and maintaining competence. So psychologists provide services; they teach and conduct research in populations in areas within the bounds of their competence -- that's a requirement -- based on their education, training, their supervised experience, consultations, study, or professional experience. Psychologists who plan to provide services and either teach or conduct the research involving populations, areas, techniques and technologies new to them have to undertake the element of education, training, supervised experience, consultation and study – sort of what we're doing every day.

And once again, if it is a brand new technology -- and there are technologies that seemingly come out monthly -- when those technologies are then turned around and used to render telemedicine services, you've got to think about the implications of it.

What does that mean when we look at these standards like the APA Ethical Standards? Basically, the competence standards mean the technology tools in clinical care. Well, okay, then if you're new to the technology, then you need to get a better understanding of what it is and what is done with it. And you can get that in any number of ways; but at a minimum, you're going to need to educate yourself. You should talk with your colleagues, talk to your supervisors, and bring yourself up to speed on this and try to think through the implications and uses.

So I noted earlier, just the simple concept of using e-mail; and it's something that continues to be of interest to providers of all sorts – not just in psychology, for example – about what are the things that we need to be concerned about. So from a legal perspective, the analysis goes all the way from don't worry about it to the worst possible outcome; and so that would be a death of some sort – either of the patient or the client or of someone else – how that could come about. So typically when we're talking about psychology, we're looking at suicide or perhaps a Tarasoff type of issue.

Now, if you rely – well, you probably shouldn't rely on e-mail – but it would be a technology that some clinicians use. Obviously, it has limitations that we've already noted – limitations that the risk would destroy your party either as one of the submissions and narrative, somebody actively stealing information to an inadvertent disclosure, to a disclosure coming from a third party. Instead of the physical stealing, it would be using some sort of electronic means to get the information and then what happens with it.

So we recall the story that was in the news several months ago with all these actresses and models and photographs, selfies, and how this information has been publicized. And somebody illegally broke into Apple's servers; but I think there were some others that were implicated. Well, that's a risk that, again, any time information is recorded in any form, there's a risk there's going to be a disclosure. So if you're talking to a patient or client, you've got to inform them that is a very current risk that they need to be concerned about; and for some devices, they should be much more leery about using some technologies versus others.

What are some of the boundaries to competence that you could think of? Well, it changes. The technology changes, and then the boundaries sometimes change. With that, of course, is the question of how do you maintain competency with all that's going on? Well, once again, it's an iterative process; so you would go back and you would have to maintain the understanding of the technology and the limitations. Where appropriate in the Department of Defense – if you're a DoD practitioner, you will want to provide some guidance in how we use these things.

Let's say we're talking about an app that we're creating for use within the Department of Defense. So we're going to provide some support to help make sure that a provider's ability to remain competent is much easier than if they don't. So along those lines, we want to make sure that we think, for example, if it becomes part of an IT system, it has to meet IT guidelines. And likewise, if this information is being transmitted, then it's going to be transmitted in the meanings that meet the privacy requirements that the Department of Defense has put out.

Well, if we were sitting in a traditional classroom, we would have a great discussion here; but we're in a virtual discussion. And so I strongly invite you to respond to any of these questions when we discuss what we're doing. The initial question is: Are there any technologies with current limited empirical evidence that have been used effectively? Anyone?

[Pause for responses]

Any psychologist at all want to take that – or psychiatrist or social worker or technician?

Well, all right, I see we've got (inaudible) and PE Coach. We've got that. It's been used with some success. And I'm not familiar with (inaudible). Does anyone want to talk about that?

Okay, well, the one thing I would – okay, and we have another comment. PE Coach, limited empirical evidence. It's consistent with the (inaudible) used to track outcome. That's excellent. And you got very good advice. The patient was instructed to be sure to lock the phone and use a passcode with PE Coach. That's excellent advice and rich for discussion.

Any time that we're using a technology, we need to consider the risk and, when appropriate, I'm talking about communicating information to the patient, and you've got to consider advising them about the risk of the communication of it. All right, yeah, I see a lot of feedback here.

Anyone familiar with Doctor on Demand telehealth? That's a medicine psychology course. I'm not. I'll have to read up on that one. One of the things for practitioners using some of these new technologies, always interested in empirical evidence. If you've got a research project you want to envision and go through the appropriate protocols and take it to an IRB and let's see some results because this can be extremely helpful if we've got more than just anecdotal information.

Okay, yeah, I see virtual Hope Box. That's a good tool. Breathe to Relax, that's a very popular app out there. I don't know that there have been studies about that specific app; but the concept, of course, has been written about. VA Telehealth System, great results for patients in rural areas. I've talked with some VA providers, and they have been given some very specific benefits that they've had with patients.

One provider mentioned to me he had a patient to live in a very remote area, a mountainous area. It was a real burden for the patient at his advanced age and his medical condition to make it from his remote location to the facility. And the protocol that was authorized by the VA in that instance, the provider was allowed to actually interact with the patient in his home.

The patient was evaluated for risk; and it was determined that in that situation, under those circumstances, that patient was a proper candidate for that. And the provider told me it was great because otherwise – the patient badly needed treatment. And that individual patient had found that the burden of going all the way to the nearest VA facility to get the help was problematic. And the provider was concerned the patient just couldn't come. In fact, after a couple of episodes, the patient didn't want to make an appointment. This was something that was evaluated and worked in that individual case. And that's one of the things, I know providers who work in telehealth want to do to the extent that it's permitted.

Now, within the Department of Defense, we're not there yet. We have specific rules on what is currently authorized. But in the future, who knows? Things are being considered. I'll just put it like that.

So we looked at all these examples. The example I gave – okay, why was technology selected for that individual? The example I gave was a patient who had a decreased ability and willingness to drive. In that case, it was a three-hour round trip at the time; and the patient just wasn't willing to do that anymore. So in that instance, telehealth was able to provide some relief for the patient.

Okay, we had several responses on Mood Tracker and on PE Coach. So the therapist would monitor effectiveness. Most often, I think, when Mood Tracker was devised originally -- and I have no reason to believe that's not being done – but the patient or client would bring a device in and sit down with the provider and go over it with him. And that was a way that the therapist could monitor the effectiveness.

Next we see how would a therapist safeguard against harm or contraindications? Well, again, you try to anticipate this. The thing about telehealth in general, it is revolutionary; but it might not work. I had a meeting with the Pharmacy Benefits Advisory Panel, and one of the presentations noted not every drug works for every patient the same way. And there's no reason to believe that every therapy would work for every person the same way. And so if you have a therapy that you're using and there is some harm related to that, then that's something you have to consider and take steps to overcome.

And finally, how is the use of this technology different than the integration of telepsychology in clinical care? What are you doing that is different than what you have been? Those are just important things to consider.

Next.

These are very clear. The APA Ethics Standard 2: Competency Recommendations – evidence-based practices first. Always put evidence-based practices first, and that applies throughout health care.

I had a presentation recently – I attended a presentation from a health care concern that wanted to sell the Department of Defense a therapy that is not currently recognized by DoD. And they really wanted our business in the worst way and wanted to know what they needed to do to make their concern one of ours so they could do business with us, frankly. And we said, well, you've got do your research well. You've got this great idea. You think you can treat PTSD in a weekend? Show us the evidence. Do the research. And so that is critical. That's how you get the best medicine, the evidence-based practices come first.

The next point, a very strong recommendation, is practice it outside of therapy before you use it. Get to know it inside and out because your patients and clients that we have that may well be of a different generation. And maybe they're a little more technologically savvy. And they may come up with questions for you and they discover things in an app that you didn't know were there.

There have been plenty of folks that have bought cellphones or IOS devices, tablets, whatever; and they don't know everything that device can do. And obviously, if you're using something in therapy, you really should know what its capabilities are and limitations. That way you can assess the risk that's there.

And obviously, if you've done that research ahead of time, the research where you just familiarize yourself with the app before the patient is there, you're going to come off much more credibly with your patient/client rather than sitting in front of him and struggling around with the device trying to get to the point that the client or patient is wanting to get to.

And obviously education and training – it's why we do this. Attorneys are no different than doctors; they are continuing their education to stay abreast because things are changing. They're not stopped for us. Technology continues to expand at an ever increasing rate. With technology, obviously, we see how it's used in medicine. And then when we're using it specifically within telepsychology or any other aspect of telemedicine, we need to be aware of where technology is leading us so we can do the best job with the technology that we have and do so in a manner where we've mitigated the risk and we can get a beneficial result with our patients and clients.

And obviously, it's just common sense; consult with your colleagues. And if you're at an installation and you're one of only one or two or just a handful of providers, you have to consult with them; but you have colleagues elsewhere within the Department of Defense in Federal Government and outside of government that you can consult with in coming up to speed on how to use technologies.

I would caution you; when you're learning technology, that's great but still you want to consult with your jurisdiction. I say your jurisdiction meaning if you're at the Department of Defense within DoD or your service within the VA or HHS, whomever, to make sure that you're aware of any concerns that may be out there about the use of the technology.

Next.

And we talked about human relations here briefly. It's interesting to me that there are similarities in many ways with the practice of law when you have a legal client as you do when you're a psychologist with your clients. In the area of risk, you have multiple relationships and conflicts of interest. That's something that you need to consider.

The ethical guidance with multiple relationships – the guidelines point out that psychologists must refrain from entering into multiple relationships if they could be easily expected to impair the psychologist's objectivity, competence, or effectiveness in performing his or her functions as a psychologist or otherwise risk exploitation or harm to the person with whom the professional relationship exists.

The guidelines also state that multiple relationships that would not be reasonably expected to cause impairment or risk, exploitation or harm, are not unethical. Just because you've got more than one party to the situation, obviously, doesn't mean that you've entered into an unethical situation. Again, the point they make, is could it reasonably be expected to impair the psychologist's objectivity, competency, or effectiveness.

Now, so what happens when the psychologist finds out that due to unforeseen factors, you do have a problem with a potential harmful multiple relationship? Well, obviously, you've got to deal with it. So the psychologist takes reasonable steps to resolve that with due regard and to the best interests of the affected person and in compliance with the Ethics Code.

And there are different places you go to get that guidance. When a psychologist is required by law and by institutional policy – and by institution, I don't just mean the MTF. I don't mean the treatment facility. I mean the Department of Defense Services or Department of VA, Department of HHS. So that would be your institutional policy that would include that. So when a psychologist is required by law, institutional policy, or extraordinary circumstances to serve in more than one role in a judicial or administrative proceeding, at the outset, they need to clarify the role, expectations, and the extent of confidentiality in their exchanges.

I had a question just this week from an attorney at a military installation not that far from here, but they had a need for a psychologist to assist in a court martialing. And the question as we ended up discussing, it involved a conflict of interest. So we had to go to a different facility to find a psychologist that could assist the case in a different realm. Somebody ended up (inaudible), so we wanted to get a psychologist from a different MTF to assist.

So think about that. So we talked about multiple relationships. We discussed conflicts of interest. Now, how would that possibly come in the topic we're talking about today, telepsychology? How could that happen? Well, we had a case study a few minutes ago where we discussed what could possibly happen? One thing was we have an inadvertent disclosure; that could certainly be a problem.

And so now everybody wants to be on Facebook or other platforms similar. Facebook seems to be the most popular. People like to text. And 20 years ago, we talked to people about e-mail and that they have to be concerned about one you fire it, it's gone. Well, texts are more immediate it seems. It's essentially the same technology; but because it's a handheld device, people don't necessarily think before they send them. So obviously, they risk that.

So psychologists need to be aware of potential boundary issues that arise when using specific telecommunication technologies. And they're encouraged to weigh the risks and benefits in relationships with their clients when they're using these telecommunication technologies. And they should do that before they enter into the relationship and before they use the technologies in that relationship.

I talked a little bit about conflicts of interest, and that should be fairly straightforward. Again, the general rule on that – psychologists refrain from taking on a professional role, personal, scientific, professional, legal, financial, and other interest relationships could reasonably be expected; and that rule applies without regard to telepsychology or any of the telemedicine issues.

To the extent that you've got a potential conflict of guidance between departments – let's say you're a VA provider and you're rendering assistance within the Department of Defense, obviously, you need to sort that out. So you'd go to your supervisor and seek out some legal consultation if you have an issue.

So the last topic I'm going to talk about on that is informed consent. Just as we have with our clients, we want to discuss how it is that we're going to proceed through the professional relationship in everything that we're going to do. We need to disclose to them the risks of what we're doing with the technology. So if what we're doing is we're transmitting information to the Mood Tracker or to PE Coach or something like that, we need to advise them of the risks within them.

We had a provider earlier supply what he had done in his practice, and it was entirely appropriate. The patient was using an app on their smartphone, and the provider advised him you need to lock that phone when you're not using it. Lock it and protect the information.

So one of the things about informed consent in general -- I've got an activity after this. But in essence, what you want to do if you're using a new technology, you need to factor in how it is you're going to use that technology with your patient and advise them. As part of the informed consent, these are the risks that we have to be concerned with.

Next.

The APA mandates that certain things be considered, and that is: the manner in which the patient or client uses the technology; the boundaries that are established and observed, very important; procedures for responding to electronic communications from clients. Once again, the patient needs to understand that if you're going to use these electronic communications, how that is going to be addressed. So if the psychologist is not on duty 24/7, then the patient/client needs to understand that.

I attended a presentation the other day, and the vendor said we've got 24/7 services. And I'm curious, well, how can you do that? We wanted to evaluate what it is that we were buying for the Department of Defense. And so basically the client will send an e-mail to us, and we will answer the e-mail in due course. They call that 24/7; well, that's something different than what a lot of us would look at 24/7. But you need to communicate that with a client if you're going to use electronic communications, how that's going to transpire. Obviously, all of this would have to be addressed.

You need to provide the patient or the client with adequate information regarding the risks a technology may pose in both equipment and in the processes utilized with the equipment; and I already talked about that with securing information.

Next.

A few words about confidentiality – obviously, you're a provider and you know the standards that you're required to follow with confidentiality. You've got certain risks when you use electronic communications. That is, once again, you need to make sure it's secure and that you maintain confidentiality; you want to discuss the limits up front with your client, including providing informed consent. If you're going to be doing any recording, make sure that what you're doing is legal; it's not always legal. And then obviously you want to minimize intrusions on privacy.

Next.

Okay, and this pretty much applies: "My lawyer will call your lawyer as soon as he speaks with his lawyer." In my life, sometimes that's what we're doing. I've been consulting with the folks that have been doing it for years, and still we find things that none of us have ever considered.

I've got some more case examples there that you can consider on your own. But we told you that we were going to provide a period at the end of this for questions and answers. And so we're going to get to that point right now. And so we're going to open the – but one other item is the cultural considerations. I've got another topic here to discuss.

The biggest thing is, as I alluded to earlier, we've got a different generation that is entering the armed forces than our generation. Even if you're 35, a young person of 35 I now say, there are 18- and 19-year-olds that are entering the service that have a different concept of technology than what you had when you were that same age; and you need to be aware of that, and you need to discuss all that with them.

So we're going to open this for questions -- anything related to ethics, security, privacy.

[Pause for responses]

Thank you. We have some questions that have come in, and there's one that has been asked a couple of different ways. The question is: Is there a difference between e-mail and security messaging? And from a technology point of view, the risk of disclosure is different for those two. So your conversation has been mostly regarding e-mail, which does not have anything encrypted with anything being transmitted. Security messaging – the whole point of it is that when you put something in, it is encrypted. And when somebody looks at it, it's encrypted. So these are very different technologies, right?

Yes, and so we haven't had the ability to do secure messaging for as long as we've had the ability to do e-mail. And so e-mail is not protected. But secure messaging is. In fact, we've got contracts out there now that we use within the military health system for using it. And it's a great technology. I've got

colleagues who sing the praises of it all the time. Once again, you just need to make sure if you're using it that you've discussed with your client how to it's used and that it's not like you're sitting there with the computer 24/7 at their beck and call. But, yes, that's a great point. There is a difference between e-mail and secure messaging.

Thank you. Another question: You said we had to be aware of our hardware and software. How familiar do we have to be with the client's hardware and software? That's a good question.

Yes, that's great. In the world of DoD, we feel much more comfortable if people are using a platform that we've provided them. So they're at their workspace, and they've got a secure network that you're communicating with your provider on. That's probably the best possible way. But the reality is, we have our lives at work; this is just a part of it. And so when the client back is home, is traveling, or whatever and they have a question come up, well, that's part of the risk that you have to discuss with the client. If they're using their own platform that is not a government-provided device, then you just have to disclose the risk to them so that they understand what it is.

Now, do you need to know all the ins and outs of what it is they're doing? You don't have to be an info geek on it; that's not the requirement. But you probably should be aware of the risks. So we had a provider earlier that commented with respect to the PE Coach that he advised that particular client who was using it of the risk and that when using the PE Coach that he needs to ensure that the app is locked and that there is a password that protects access to it. So that was one of the risks that they were concerned about there.

I guess a related question that has been asked in a slightly different way: Is there a difference between DoD and VA developed app? And especially in terms of security – are they different?

Yes, there is a difference in apps. The VA and DoD platforms in apps have all undergone a legal review. Not that we are the sine qua non of it; but as part of that review, we do talk to our privacy people and we make sure that we've gotten their concurrence before we go forward. So to that extent, it's been vetted.

But obviously, we didn't create the wheel. And there are great technologies out there that the government didn't invent. And should a provider be prohibited from using those technologies? Well, you should probably know those technologies are out there. And if there's something that's really great that you want to use as part of your practice, then I would say take it up with your colleagues or your supervisor and forward it up. If you want to use a new technology that was never developed before, let's take a look at it and decide how and if we can take advantage of that technology.

Before I came here today, the conference that I was at immediately preceding this was with the Interagency Program Office. And they have a virtual sandbox. And when they find applications that the clinicians want to use, they put it in the sandbox and they test it and they give it a security rating. So we're to a point where we can at least give you a list of things that we've tested and we know that these are safe to use.

We didn't invent them, but we did two types of testing on them. We tested them to make sure that the (inaudible) is good, and then we tested them to make sure that the way the information is stored is safe. And so we can at least say that there is nothing malicious in the way that it's designed, and there's nothing that is of concern about the way that the information is stored. At least we can do that for people. And so I guess I was excited in the Interagency Program Office that if people have questions, at least now we have a way to answer that question.

Yeah, that's great. I was talking to Dr. O'Donnell before we started today. DCoE used to be part of the TRICARE Management Activity, which was where I worked before. It morphed into the Defense Health Agency. And DCoE will be coming back, and of course the Integrated Program Office also has very strong links to the Defense Health Agency and we looked forward to working with DCoE in the IT area when DCoE comes back to DHA.

We have a couple of questions about protection for the clinician and standards for the clinician. So one of the questions: Are protection standards regarded as the same under UCMJ and civilian courts?

Great question and it's not an easy one. We could probably spend a couple of hours talking about that. We won't do that this afternoon. In general, the advice I would give you – and particularly within the area of psychologists as opposed to MDs – I know the APA has issued several position papers on this subject; particularly like the use of psychologists in employed settings and more specifically, in interrogations and such. And so there have been some resolutions from DoD and how those are going to be handled in that situation.

But in general, we strive not to have things as confusing as possible, despite what my previous slide about lawyers indicated. In our military standards for providers and beyond military, our DoD standards with providers, we try to follow as much as possible very similar standards with what we have in state jurisdictions. However, just as not every state follows the same exact rule for every incident, certainly the DoD standards are not necessarily the same.

So there may be some areas that we might move to a different answer on. I can tell you specifically also in the law, we use the same thing. I'm a retired Air Force JAG. We tried lots of court martials; all three different sides of it – as a prosecutor, (inaudible) and judge. And we had different rules than civilian jurisdictions on a few interesting points.

The most common example that would be analogous to what we'd have in psychology would be like the Tarasoff situation. That's when you have -- Tarasoff was a patient/client who had expressed that they were going to harm another person; they were going to kill someone. And we've got specific rules in the military that are maybe a little bit tighter than you would have in civilian jurisdictions to help you arrive at that answer.

In general, they're going to be very similar, but if you've got a tough question, then I would advise you to seek guidance. Each of the services have some talented legal practitioners who could help you to get to a legal answer, what you need to do to make sure that you are consistent with what the military departments expect of you, the DoD. As well as we'll also give you some advice as far as your state jurisdiction.

I know we've got one attorney in the Air Force, who is a seasoned health care attorney, who has practiced for over 40 years and knows his stuff better than most. He and I still talk on tough issues.

So I would say, seek out the guidance when you get the hard, specific questions. See if you can get the best advice possible. In some instances, obviously I know it came up with respect to (inaudible) matters on there. We had providers that sought out guidance from their state authorities. And if that is in conflict with a military setting, then ordinarily we want to advise you to follow up with a military department.

However, there are some very problematic areas. We try to avoid putting people in a situation where their license might be at stake. In general, that's not what we want to do. That's not what you got into the profession for.

Thank you. We have had some really excellent questions. I'm really sorry we can't get to them all. But I would like to close out with one, which is: Are there any protections for the clinician in the event of a patient recording a session without the clinician's awareness. If using a concealed recording device, et cetera, what happens in that instance?

Okay, what privacy protection does the clinician have? That's a good question. Most of us here probably remember the whole Clinton/Lewinski fiasco. And the way that ultimately came about was that there was a recording made of a conversation between a civilian employee who happened to work at the Pentagon and Ms. Lewinski. And in the jurisdiction where it occurred, Maryland, that was an unlawful use of technology. And so despite what Monica Lewinski may have wanted or didn't want, the prosecutor in that

jurisdiction decided to go ahead and see prosecution. Ultimately, the case was addressed outside of court.

But in some jurisdictions, there is a specific prohibition against surreptitiously recording conversations. Not every jurisdiction follows that rule. In most jurisdictions, the rule is at least one party has to consent to it. So that's your problem; you've got a client who came in with a recording device and is surreptitiously recording. In some jurisdictions that may be permitted; in some, it would be obviously unlawful, like we talked about.

What I would advise you is to be an active consumer. It shouldn't be hard to find out what the law is in your jurisdiction. In addition, within the military, there is probably not going to be a specific prohibition against it. I'm aware of at least one case where an alleged victim recorded her alleged perpetrator; and ultimately, she ended up trying to blackmail him. So they both ended up getting in trouble in different court martials, which was unfortunate. But sometimes, that's a little bit far afield than what you're getting at.

How do you protect against that? I think it's the same thing that you enter into with any client. There's got to be trust in the relationship. You're going to be professional and do everything you're supposed to do. But is it necessary in the protection to get beyond that? Unless the state provides it, there is not specifically a rule that's going to prohibit that.

I'm aware; I think we had that issue come up in court personally. I saw something in the media about it. There was a patient who recorded – I think it was a mental health practitioner involved in a case. And when they turned that recording over to the IAG.

So how do you prevent that from happening? In that instance, there wasn't a legal way of doing it. You can always ask up front. Here's part of what we do here; this is about trust. I don't record; you don't record. If that's something you need to do, if you have to have that conversation of course, then that's the whole trust thing too. The fact that they may be surreptitiously taping you, maybe that's not the best relationship you've ever had as a provider with a patient.

Lots of thought provoking questions – thank you so much.

A reminder, after the webinar, please go to www.continuingeducation.dcri.duke.edu to complete the online CE posttest and evaluation and download your CE Certificate or your Certificate of Attendance.

Thank you again to our presenter, Mr. Wheeler, for today's presentation. This will be archived in the Monthly Webinars section of the DCoE website.

To help us improve future webinars, we encourage you to complete the feedback tool that will open in a separate browser on your computer.

To access the presentation and resources after the webinar, visit the DCoE website at www.dcoe.mil/webinars. An audio podcast and edited transcript of the closed captioning text will be posted to that link.

The Chat function will remain open for the usual 10 minutes after the conclusion of the webinar to permit attendees to continue to network with each other.

Please save the date for DCoE's April webinars: Traumatic Brain Injury webinar, Prevention and Management of Concussion/mild Traumatic Brain Injury in Youth Sports, April 9, 2015, from 1:00 p.m. to 2:30 p.m. Eastern Time; Psychological Health and Resilience of Children in Military Families: How Child Narcissism Impacts their Development and Implications for Clinical Practice, April 30, 2015, 1:00 p.m. to 2:30 p.m. Eastern Time.

Thank you again for your attention. Have a great day.