Telehealth Learning Series Top 5 – Episode 2

NARRATOR: Hello and welcome to Top Telehealth Tips and Lessons Learned, part of the Telehealth learning and discussion series for substance use disorder treatment and recovery support providers. This project is brought to you by the Addiction Technology Transfer Center Network, the Center for Excellence on Protected Health Information, the National Consortium of Telehealth Resource Centers, and the Center for the Application of Substance Abuse Technologies at the University of Nevada Reno, in response to the COVID-19 pandemic.

Today's speakers are Christine Khaikin, Jacqueline Seitz, and Michael Graziano from SAMHSA's Center of Excellence on Protected Health Information. This expert group discusses the top seven privacy considerations for Telehealth during COVID-19. Welcome to the show, and let's get started.

CHRISTINE KHAIKIN: OK, great. Hi. This is Christine Khaikin. Nice to see everyone. So our first key point is just that you can still take action to protect client confidential information, and this is really important because Telehealth may increase both the number of people, and technological systems, and different companies that could have access to confidential health information. And you know, we've mentioned this throughout a lot of the other subject matter experts have mentioned this, but providers should really focus on themselves as well, avoiding public Wi-Fi, password protecting devices, keeping files secure both, you know, from your family and also on your computer if at all possible.

So this is, we've talked about this a little bit. This is really important here. You can use widely available apps to support service delivery right now. The Office of Civil Rights, in their guidance, announced that they are going to waive potential penalties for HIPAA violations arising out of what they're calling good faith use of Telehealth. They have listed in their FAQ to a link to-- I think it's linked here-- apps that can be used right now. So that does include things like FaceTime, or Skype, or Zoom, or other texting apps. But I think a lot of people have pointed out that it's good to keep up good habits also and whether there are going to be penalties or not is not the only consideration for your clients' privacy.

So if possible, you can use different things. Some of that, Google Hangouts, that is listed. We'll show the link again. SAMHSA has also released guidance. And what they have said-- so they've emphasized that providers can make their own determinations as to whether a medical emergency exists. Part two currently permits disclosures without consent for medical emergencies when patients' consent cannot be obtained. As we talked about, not everyone is able to do an e-signature or an electronic signature.

And so the example here is medical emergency may exist when someone needs substance use disorder treatment services but consent cannot be obtained because of the COVID-19 pandemic. As we said earlier, providers should be documenting any disclosures. They should be keeping in mind that records disclosed under the exception no longer received part two protections unless they've been disclosed. And also, importantly, this exception applies to disclosures for treatment purposes. You still need written patient consent for billing purposes, and I did speak to at least one provider who was going to be holding submitting claims until they can get that written

consent in person. But that's something to think about. [INAUDIBLE] I'm going to turn it over to Jacqueline.

JACQUELINE SEITZ: Thanks, Christine. OK. So let's talk a little bit more about in-person consent. As we talked about at the beginning of this call, in-person consent for authorizing disclosures of substance use disorder treatment information is not necessary. Part two accepts electronic signatures on consent forms. And again, we're talking about consent to disclose information. We're not talking about consent to treatment. Part two doesn't say anything about consent to treatment. We're talking about the sort of consent forms you get when you sign up a patient and you want an emergency contact. So you want to be able to contact their emergency contact and to bill insurance.

So part two permits e-signatures. And someone asked at the beginning, you know, a very creative question about using whiteboard and Zoom. Part two only says e-signatures are permissible. There's no additional guidance. I think at this point-- and I'm trying to speak very carefully because I'm not giving legal advice. I'm just sort of trying to speak common sense. At this point, if the regulations say you can't do it, then you shouldn't do it. But if you're coming up with a creative solution as a stopgap and later you're sending a physical consent form through the mail that the person can sign and send back. You know, if you're helping save someone's life by providing substance use disorder treatment, I find it hard to imagine that there would be an enforcement action right now for violating the e-signature provision of part two.

The important thing is is the client or patient understanding the terms of the consent form? So if you scroll through the whole consent form and they've understood to whom they're disclosing the information, and then they sign with your creative whiteboard solution, it's hard to imagine that the patient later complaining because they would have known that they were authorizing that disclosure. And again, in the sort of current enforcement scheme, I—uh, well, I won't say anymore. But I think creative solutions are, you know, what we need right now.

Let's see. The other thing I want to highlight here is that when you are disclosing pursuant to patient consent-- so let's say that you are billing insurance or you're contacting their emergency contact, you always need to make sure that you're including a notice prohibiting re-disclosure on those documents, and that notice can also be electronic. So it doesn't need to be paper. It can be an email or any electronic media as long as it's written. And finally, providers should always obtain consent to disclose to the Telehealth service if the Telehealth service-- whatever communication service is your thing-- is going to have access to the patient information.

Let's say, for instance, that you're using a hypothetical service that we know is monitoring all of the text information and putting that into an algorithm that they can market later like need new sneakers. If they're reading that information, then you'll need patient consent to authorize the disclosure to them, right. Because you know that someone somewhere is reading that information. So that's something to keep in mind, and that's the beauty of using encrypted, end to end encrypted services, because you know that the Telehealth provider doesn't have access to that information. And if we have time, maybe our Telehealth experts can speak a little bit more to that issue.

Check your state laws. If there's a state law that has a more protected privacy protection, then you need to follow the state law on top of the federal law. Mary Ellen pointed that out very nicely a few minutes ago. I'm just going to keep speeding through because we're running out of time. The same protections that you're thinking when you're working remotely-- keeping your Wi-Fi secure, keeping your files safe, making sure people can't overhear you-- all of those also apply to your patient. Again, Mary Ellen spoke very well to that point a few minutes ago, and the Center of Excellence is working on creating a resource that providers can give patients to help patients understand the steps that they can be taking to maintain privacy in their own setting. Oh, and so this is the same point with clients can protect their information. Again, we're working on a resource. And now I'll turn it back over for the remaining three minutes to Michael.

MICHAEL GRAZIANO: Thank you, Jackie. So the COE-PHI is a partnership between CAI of the Legal Action Center. We're here to help with your questions related to protected Health Information and federal privacy laws. Here's how to access our services and resources. Please visit COEPHI.org where you can ask individualized technical assistance and also view our resource library. The resources and services that we provide do not constitute legal advice, and we thank you all for joining us today for this presentation.

NARRATOR: Thank you so much for joining us today. For a transcript of this podcast, presentation slides, and other related resources, please visit our website site at www.TelehealthLearning.org. This podcast is supported by funding from the U.S. Department of Health and Human Services, Substance Abuse and Mental Health Services Administration, and Health Resources and Services Administration. Its contents are solely the responsibility of the presenters and do not necessarily represent the official views of HHS, SAMHSA, or HRSA. Information shared and views expressed reflect the speaker's best understanding of science and promising practices and should not be seen as directives.

We encourage all listeners to reflect on the context discussed during this series and to take that information to colleagues and/or supervisors for further discussion, especially in the context of state rules and regulations. In addition, content related to privacy and security and 42 CFR part 2 presented during these sessions should not be construed as legal advice, and listeners are directed to discuss recommendations with their agency’s legal counsel. Finally, listeners should consult SAMHSA resources that provide additional information regarding delivering services virtually. Once again, thank you to our listeners for tuning in today. We hope that you'll join us again.