AUA Inside Tract Podcast Transcript
Episode No. 92

COVID-19: Understanding HIPAA Relief Provisions for Telehealth

Host: With the Covid-19 pandemic, the federal government has taken a number of steps to make it easier to adopt telehealth practices. Today, we're talking with Alisa Chestler with the Baker Donelson law firm to discuss new guidance and waivers regarding HIPAA as it relates to telehealth. Alisa, we understand the government has released new guidance around this issue. So, what documents and waivers are currently in play, and can you give us just some key takeaways that practices need to know about, and what's changed, and what's staying the same with telehealth?

Alisa: The federal government has issued several different guidance and frequently asked questions or FAQs with respect to both HIPAA and telehealth. The most important piece of information is that, specifically with telehealth only, they have stated that they will waive enforcement of certain privacy, security, and breach notification rules. So, what does that really mean? That means that as doctors try to see as many patients as possible during this time, and they do so via telehealth, they can do so with some assurance that they do not have to operate in, let's just call it, a perfect world. While they should take strides to ensure as much privacy as possible, certain portions of the privacy rule, for example, they understand, are going to be difficult to provide.

One example of that is a notice of privacy practices. Every day when a patient walks into an office, they're handed intake paperwork and in there is your notice of privacy practices, which is the document required by HIPAA, explaining how the practice will use and disclose protected health information. We're informing telehealth at this time, and this time only, you do not have to worry about ensuring that the patient receives that notice and acknowledges it in paper.

The second part to that is certainly the security of the system. What HHS or OCR, the Office for Civil Rights, who enforces HIPAA has done is in this waiver, they have also cited certain methodologies of telehealth that are acceptable and a few that are not. So, as physicians are considering moving to telehealth, they should absolutely take a look, figure out if the methodology that they're considering using is on there. And one part of that is, as you know, you're supposed to have a business associate agreement with all of these platforms. If you do not secure a business associate agreement at this time, OCR has stated they will not, again, enforce obtaining that. But I will say, as a

word of caution, not to take this at carte blanche because the rules will revert back and you will then have information with a third-party provider that's not under a business associate agreement.

So, what I would say is that as physicians consider moving to telemedicine, and do so quickly, it's fine to do so without that business associate agreement in place. But you really do need to be thinking about putting one in place sooner rather than later and probably before the pandemic's done to ensure that the information that you're maintaining and retaining is under control if you will.

And the lastly is that breach notification rule. As some of you may know and read, there are breaches that are occurring on a daily basis of both large entities that you read about in the press, but so many smaller entities that just don't make the headline news, including physician practices. So, I would certainly caution on that breach part in terms of realizing, yes, indeed there is some waiver as it relates to that enforcement. However, there are state laws that providers still need to be cognizant of.

Host: Do these waivers apply to telehealth for both the new patients and established patients?

Alisa: They do. And what's great about that is that you can be seeing lots of new patients for a variety of reasons. But I would, again, caution physicians seeing patients that they don't know. So, for example, while some of the HIPAA issues have been waived, other issues haven't. And we still see from time to time medical identity theft in the system. And you really do need to ensure that for new patients, you are paying very careful heed to ensure that the person that you are seeing is the person that you will be charging. Or at least you have, again, the right policyholder. So, generally speaking, at the time of initiating that first visit, you need to figure out what your methodology is going to be for validating that you are seeing the right person and creating a medical record for that right person.

Host: What advice would you have to practices that are jumping into telemedicine for the first time, right now, during this pandemic?

Alisa: I would definitely recommend doing one or two, what I'll call, test runs. Practice on your brother-in-law across the country, practice on, you know, a friend on the other side of the street. Make sure not just that the technology works, but make sure that you also understand what information you're going to be getting, and where you're going to be gathering it. It's probably not a good idea to keep a notebook next to you and just start jotting notes in there because you've then got a lot of paper PHI or Protected Health Information. So, we

would recommend that you figure out what you're going to do while you're on that call in a few different scenarios. Even with just starting, how are you going to initiate that call? How are you going to make sure that one patient doesn't see another patient if you're using a slightly more sophisticated technology? So, I would certainly try to make sure that you get the feel for the flow of a telemedicine visit before you actually do the first one that you're planning to charge for.

Host: What other special considerations do you have for practitioners when it comes to data security right now?

Alisa: So, a couple of things. As I mentioned earlier, providers are still open to a cyber issue and cyber attack. We are still seeing ransomware in the industry. And so while HIPAA has waived certain breach notification obligations, if you put down your defenses, if you start to utilize unsecured technologies, and if your information were to get locked up, while you may not necessarily have a breach notification rule under federal law, again, you're still going to have state law issues. And in most ransomware attacks these days, you are not going to have access to either your EMR or other databases that contain and retaining information that you need. Right?

So, don't loosen your defense so much that you've become vulnerable. We have seen with a shift to telework in general, that the criminals are looking at this as an exposure point to just gain a little money, and they are still going after the healthcare industry. I know I've read some news accounts where maybe they're laying off and leaving hospitals and some providers alone. That is true in some places, but we've just seen that a hospital in Paris was recently attacked. There are still smaller U.S. practices that you're not reading about that are getting hit with ransomware. So, just because you may not have a breach notification requirement under federal law does equate to loosen up because again, you're still going to have your state law requirements, and you still need access to your record.

Host: You mentioned unsecured technologies. What are some examples of those that you would recommend people kind of steer clear of?

Alisa: You know, I would say it's those that are not, I don't want to necessarily mention any, particularly by phone, right, that I haven't really tested out. But I will say that those that are not on the list and the waiver is very easy to obtain. If you can't find it, your attorney should be able to find it with no problem on the Office for Civil Rights website. It lists a lot of very good technologies that people are switching over to. I'll note that Google Hangout is one that is on the list of approved methodologies. So, there's many that are. And how are they

unsecured? They are permitting certain communications that are not secured in the same way as this. We all have home Wi-Fi, right? Hopefully, people's home Wi-Fis are secured and not open to their neighbors or people driving by. The same would be true for this technology.

Host: Gotcha. And what kind of flexibility are these new measures providing for physicians overall? And what does this mean for licensing across state lines?

Alisa: All right, so, ladies and gentlemen, licensing across state lines still exist. Okay? There are states which are waving these, but it's on a, what I'll call, a one-off-like basis. So, we are certainly monitoring state by state how they are permitting providers from other states to provide care to patients in their particular state. As you know, we are having doctor shortages in certain hotspot areas. And as physicians, you are hoping to help in those hotspots and certainly, the state regulators know that. So, most of them certainly are providing relief as it relates to practicing medicine across state lines. But I would certainly caution you, and again, tell you that it's a good idea to double-check in those states that you intend to provide some treatment and if it's over and above the states in which you currently have a medical license. The same, by the way, is true for some of your paraprofessionals. And I will note that the federal government has also issued some guidance in this area, and it is, in general, helpful to the cause of seeing as many patients as a physician is able to see in any one time

Host: In the future, and we all hope the near future, medical practices will return to their old normal. So, what happens at that point?

Alisa: So, what we would expect to see is directives from the federal government in particular in which they say we're going back to normal. And you know, we'll all probably start to become aware of that whenever that is. We'll all hopefully be returning to our respective offices, and hopefully, going out to restaurants and all the like. And at that point, I would say to physicians who very much might like telehealth, might like the flexibility of telehealth to remember that a lot of the practices that they may put in place today will change. And so, they need to make sure that as they loosen their belts a little and enjoy some of the, I'll call, freedoms of these waivers, that they need to make sure that they are cognizant and smart not to fall into a situation where the waivers are gone, and they are still practicing under the current rules. So, by example, I mentioned earlier in this call about notices of privacy practices, and not necessarily having to provide them, you know, at the first telehealth today, I would still, to the degree possible, try to get those to patients in advance so that you're not having to change your practices later on.

Host: Any other takeaways for our audience with regards to what we discussed today?

Alisa: Like any other operation or workflow, try to do some documentation of what you are putting into practice so that as you continue to do it, and as you formalize it, you have the underpinnings of that workflow, that you make sure that you're doing the same general workflow as any of your partners or paraprofessionals. That you know where all the information resulting from those visits are going to reside so that you can then bill them appropriately. Consult your attorney to make sure that they have assisted in helping you to develop practices that will, again, serve you well during this time and hopefully develop and grow after Covid-19 has hopefully left the country.

Host: Alisa Chestler has been our guest today on the "AUA Inside Tract" podcast. She's with Baker Donelson law firm, and we'd been discussing the new guidance and waivers regarding HIPAA as it relates to telehealth. Thank you so much, Alisa, for joining us.

Alisa: Thank you.