Tammy McCausland:

This is Tammy McCausland bringing you SROA Soundboard, SROA's podcast for radiation oncology administrators. I'm joined by Axel Wirth, chief security strategist at MedCrypt Inc. A San Diego based company that provides proactive security for healthcare technology. Welcome, Axel.

Axel Wirth:

Thanks, Tammy, for having me. Appreciate the invitation.

Tammy McCausland:

Could you tell me what kinds of cybersecurity risks exist with the increased use of telehealth because of COVID-19? (0:30)

Axel Wirth:

In general, I would phrase it that we have deployed a lot of telehealth capabilities and definitely increased our attack surface. That's very simply put. We have deployed this telehealth infrastructure in a hurry, which most likely means that we have paid less attention to security and privacy than we should have. I'm not saying that that was wrong. We certainly were under pressure that we had to react, but at the same time, we do need to be aware that clearly we made some security compromises here. We should also always consider that there are two ends to the telehealth offering, where there's the patient's side, and most likely the patient will use their personal devices at home maybe with a doctor or hospital provided application, but it is still their device and their infrastructure. On the other hand, we have the clinician who may work in a hospital or in a facility, but also maybe at home as well. So we have the two ends that are now more exposed than our traditional IT infrastructure.

Tammy McCausland:

So what are some common mistakes that happen, in terms of people not being as aware of the data privacy and the security, because we've been in a hurry? (2:00)

Axel Wirth:

I think the common mistakes are that we really have not had time to vet this new infrastructure and think through what does it mean from a HIPAA perspective? What does it mean from a state law perspective? Because most States in the US now have their own privacy and security laws in addition to HIPAA, and we may not have put the right legal protections in place. Like for example, business associate agreements with whoever is the telehealth provider we are using.

Tammy McCausland:

Now that we've been in this telehealth space for almost two months, or probably at least a month, what can oncology providers do to make sure that they're following up on the data security in the patient privacy side? (2:54)

Axel Wirth:

Yeah. So one activity is certainly on the contractual side. Make sure that whoever you're using as a telehealth provider is willing to commit to the HIPAA requirements and is willing to sign a business associate agreement. That's the contractual side. On the technical side, I think we should assure that both data at rest, as well as data in motion; as it travels the wire from the patient to the hospital, is encrypted, is protected. Or data does not reside, let's say, on the patient's device. Or that there is maybe only temporary storage and then the data is removed from the session. So either, again, encryption or data removal, but certainly encryption for data in transit.

Tammy McCausland:

How can the providers make sure that the data is being removed on the patient side? Especially, because as you said, they will be using their personal devices. Say they record a session and they want to go back to it afterwards if they're getting a lot of information. How can the providers make sure that they're not keeping the information too long? (4:07)

Axel Wirth:

Well, so the information on the patient side, I think that is a function of whatever software application is used for teleconferencing, and that, again, that application should have a function that would remove the data. Or if it is kept, at least encrypted. That's the patient side. On the clinician's side, obviously there could be indeed infrastructure available that is sufficiently protected and that is sufficiently HIPAA compliant where indeed the session could be stored and could be reviewed at a later time. There's no difference compared to that scenario, as for example, an extra MRI image you keep in your data center. So that is indeed possible to keep data on the provider side properly secured and HIPAA compliant.

Tammy McCausland:

Okay. How can administrators plan for a potential data security breach? (5:26)

Axel Wirth:

I think the fundamentals here are really to understand where your data is, which actually goes with the previous point we just discussed, how your data flows, who has access to it, and how is it protected? You need to understand these three things; location, the traveling of the data, and the protective measures of data. Of course, verify and also audit and make sure that it is indeed the way you think it is. At that point, you have enough control of your data that should a breach occur, you can quickly; A, assess the impact of the breach because you have the knowledge in need for that, and then also quickly remediate the breach and minimize the impact.

Tammy McCausland:

Given that everything's happened so quickly and people probably signed contracts, and you as you mentioned, and may not have made sure of all this important stuff. Do you think administrators can go back and review the contracts and ask for an addendum to be added or will they need to maybe find another vendor? Especially if this telehealth becomes a new norm. (6:24)

Axel Wirth:

I think most likely the former then maybe the exceptional case where indeed a given telehealth provider may not be willing to sign, for example, a business associate agreement. Then, yeah, it may require that the provider looks for a different service offering. I know that some telehealth providers provide the business associate agreements out of the gate when you set up the service with them, it's part of their default, others are more reluctant to do so. Certainly, we should be careful about more consumer-focused services, like for example, Skype or FaceTime because they typically don't have the right security controls in place that would assure HIPAA compliance. Even though for the time being OCR will exercise HIPAA enforcement discretion for telehealth, I think it's still a good practice to try to comply as much as possible in the current situation.

Tammy McCausland:

Do you think that the telehealth providers were ready for this situation we find ourselves in? (8:02)

Axel Wirth:

I think from a compliance perspective, there were certainly some out there that were ready. I think from a capacity perspective, we have seen some challenges in the onset. That all of a sudden rather than having a hundred patients a day, they had 10,000 patients a day. That was an increase in volume that technically they were not prepared for, and they had to expand their own infrastructure to support that. But I think we are past that. But from a security compliance perspective, I think there were several out there already that understood and complied with the HIPAA requirements, and were willing to provide the compliant service. I don't think that that has changed much since then.

Tammy McCausland:

Do you think the telehealth provider marketplace will get more crowded or more competitive because of COVID-19? (9:06)

Axel Wirth:

I think as a consequence of this move towards telehealth, we will see that a good amount of that will stick and many patients will say, "Well, wait a second. That worked just fine, so why should I go back and sit in traffic, find parking, visit my doctor in the office?" So I think patients will expect that at least a lot of the services will just resume via telehealth. Clearly, that will then create a market opportunity for some telehealth providers and will probably increase competitiveness, but also will create a certain shakeout. In a sense that larger companies will buy into what until now was only a niche space, but it's now much more attractive from the business perspective.

Tammy McCausland:

Will it increase the rigor for the things like the HIPAA compliance and the state laws that may be some providers are not up to par on? (10:12)

Axel Wirth:

I would expect that. I think as the opportunity grows, I think we see more professional offering across that space that indeed will understand and properly implement the security requirements needed.

Tammy McCausland:

Do you have any final thoughts or tips for administrators to make sure their center's telehealth services are up to par? (10:42)

Axel Wirth:

Well, I think we need to understand the full spectrum of the risk, and some of that is legal contractual compliance. I think [inaudible 00:12:23] to have the right partners in the organization or outside of the organization to help navigate that. Then the other side of the equation is purely technical, but it is data encryption, is data flow analysis and things like that. And again, I would hope that most administrators have the right technical resources available either within the organization or contracted with them to help them navigate the technical decisions and the technical assessments, because I think they are probably beyond what your typical administrator understands from a technology perspective and IT perspective.

Tammy McCausland:

Okay. I thank you for your time today. It was a pleasure to talk to you.

Axel Wirth:

Okay. Thanks for having me and including me.

Tammy McCausland:

Thank you. Bye.