Anne Genge - Paper versus Digital Record Keeping: What's Best for Dental Practices?

Chiraz: Hello and welcome to CDA Oasis, my name is Chiraz Guessaier. Today, I have the pleasure to speak with our Oasis friend Anne Genge, CEO and co-founder of Alexio Corporation. Anne usually talks to our viewers about cyber security and mitigating risks, security risks that dental practices may face. And today, we are speaking about paper versus digital dental records. Although numerous dental offices have now adopted digital patient records, we received a question about the benefits as well as the risks of using both recordkeeping approaches. So, Anne thank you very much for taking the time to look into this question and responding to it.

Anne: It's really great to be here always. And, I'd love to share a few slides just to go through the, the differences for you.

Chiraz: Perfect. So, before we go into the slides, for the benefit of our viewers, the exact question that came our way was, what is the difference between paper and digital dental records? And what are the risks that dentists run when using digital dental records? Also, the question included an inquiry about some of the solutions that dentists can implement to prevent the loss or hacking of their files. So, as you prepared the slides, let's go and see them.

Anne: Okay, fantastic. As you just, you know, so well said is that most digital or most dental practices have already moved to digital in one form or another. I think with the cyber climate, the way it is today, it's very easy for us to sort of have a wish that we could go backwards just to paper, but paper records had their risks also. Sometimes a chart would get lost, they didn't fare well when it came to fire and flood; and really digital records, if they're backed up properly, will always be available to us. And you know, there are a lot of glitches sometimes in transferring from the paper into the digital era. But the hiccups generally have been well worth it for a few reasons.

Anne: So, the first one, and I think that's the one, it's the leap that most people made first and that was to move towards digital x-rays and digital x-ray provided us exponential benefits when it came to diagnostics. The speed in which we were able to access information, case acceptance and treatment planning for sure. The digital records are taking up a lot less space. Instead of having walls of charts, we can move towards having everything into a small black box that we call a server. Now today, we still have people working in both. Some people have their digital x-ray and their practice management system running and they're still making notes in charts that sit on walls. But there has been much more effort to move towards the chartless or paperless charts. We have a lot more access to information in the digital record. We can search things quickly, we can transmit it between practices quickly, things like x-rays to a root canal, treatment planning back and forth from orthodontic offices. And so that's a real benefit as well.

Anne: And of course, with all of these things considered, productivity has gone way up, which is great. Now, there is a downside. It's a downside that most people are concerned about. We've talked a number of times here on Oasis about things like ransomware. It's come up a number of times with people that have written in or come to me at those terrible times when their offices have been locked down by this nasty thing they call ransomware, which is really encrypting your data. Nobody wants to be hacked, but that is a risk. Data theft can happen not just externally, but internally as well. Fraud is always on people's minds and system failure. Human error has a big factor when it comes to a number of these things, whether it's just people acting naively or sometimes in a sinister way, but it goes right through from our staff to even the outside people that are supporting us. These are all things that we have to take into consideration.

Anne: So, we have spent a number of years working in dental practices when it comes to securing data. And I'm just going to share with you here what is our blueprint and as you can see here, there's a number of things I don't want you to get scared by them, but the main point is that cybersecurity is a journey. It's not just one or two things. It's not a product that you go by and you install it and then everything's fine. Again, there's ongoing things that we need to be thinking about and you know, it really starts with deciding what are our policies for data in our practices and system use. A dentist will have feelings about that themselves, but there's also compliance issues and those things need to be put together in creating your policies and your best practices and your staff should be trained to that and you want to do that not just for compliance, but you want to protect your business in general.

Anne: And that will really help. You need to set the tone for that. A lot of those policies and a lot of the training will center around or should center around email because email is the number one way that bad stuff gets into your practice or bad guys can get into your practice. And we also want to make sure that we're protecting patient information when we're sending it out. So, we need to be looking at encryption. You do need to encrypt the email or a CDA has a beautiful program, the Secure Send, that's a great option for transmitting patient information as well. Of course, we want to make sure that we have proof from our IT company that we have good network security, server security, and workstation security in place and it does go beyond antivirus. It's something that needs constant attention and if you're just getting updates and maintenance once every six or 12 months, that's not going to be enough.

Anne: But fortunately, there's a lot of automation that can make that happen for you now, subscription-based stuff that can use automation to make sure that these systems are kept up to date on an ongoing basis. Backup, we can't emphasize enough how important backup is, but it's also really essential to test those backups. So, I have been part of a number of cases where a dentist has tried to restore their system either because of a ransomware, a system failure, and only then are they finding out that the backup was no good. Sometimes it was misconfigured, sometimes the data had some, some sort of corruption awhile back and it was never tested to make sure that it was recoverable at the time that it was needed. So, this is worth making sure that you spend a bit of money and do a fire drill, take a few hours to shut the server off, take your

backup and try to restore it and make sure that everything is there. That's the way that you're going to know.

Anne: I have assessed systems, I have it, kind of at the top and at the bottom. And that's because this is something that in many provinces it's a requirement each year to have what's called a security risk assessment. You want to have that, not just because it's a compliance issue, but because that's the way that you find out where the holes are and the gaps in your systems and your network. And it's an excellent idea to have a third party do this for you because the people that work in your systems on a daily basis, they do have blind spots. And over time, sometimes holes can get punched in the network and you want to find those and close those up. So, that's a great idea as well. So it's really, it's an ongoing set of things. I don't want people to get too overwhelmed. I'll always make myself accessible to ask questions about this, of course. And we'll even include some more information in the slides that can be downloaded after the video.

Chiraz: Anne, as usual, thank you very much for your time and expertise. I really appreciate it and it's always a pleasure to host you on Oasis.

Anne: Thank you Chiraz.