Medical Practice Trends Podcast #20

Medical Device Regulation and EMR, with guest Mike Meikle, Hawkthorne Group

Peter: This is Peter J. Polack M.D. with another Medical Practice Trends podcast. Our guest today is Mike Meikle of Hawkthorne Group, a Richmond, Virginia consulting firm. Welcome, Mike.

Mike: Hello, Dr. Polack.

Peter: Our topic today is Medical Device Regulations and EMR and this new FDA regulation known as MDDS. Can you explain what that is and how this can potentially impact medical practices?

Mike: Very recently, the FDA published what is called the Final Rule on Medical Device Data Systems. This was in February of this year. The rule is already effective. Basically, what the FDA is trying to do is update its regulation of not only medical devices, but the actual data systems that interconnect with them.

Since medical devices are becoming more and more internetworked not only with, say, themselves – data that's displayed on the unit – but also it's being put on the network, it's being put on storage, the data is being sent to additional medical devices, the FDA is trying to address all this technology that's being wrapped around these machines that, at one time, were standalone but now are being networked across the enterprise and are actually riding on the enterprise network.

Peter: It makes them a lot easier to use, obviously.

Mike: Right. This is occurring because practitioners want immediate access to data that's being captured by these systems to improve patient care. Unfortunately, with that immediate access and where the data is being collected, transferred and stored, there are some risks that are being incurred.

Peter: Basically, what they're saying is that if you have some type of diagnostic equipment that's now linked to your EMR system and you're probably storing some of these images or maybe even just pulling them up on a monitor in a different room, in essence, now the EMR system has become a medical device which the FDA is regulating.

Mike: That's correct. It's not only EMR, but the network that it travels on and where the data of that is being collected is stored.

Peter: What do you think their motivation is for doing this?

Mike: My thoughts, based on the research that I've done – and they, of course, have not said why other than it's significant patient safety issues that they're addressing because of why they put this MDDS out there – my thoughts are because of the issues that have historically faced medical devices in general, at one time medical devices ran on proprietary operating systems, if they even had an operating system, and were just standalone.

Then, of course, within the last, I'd say, ten years, medical devices have become more sophisticated and now they're running on commercially available operating systems, such as Microsoft Windows. Well, this opens up additional functionality and capability. It also brings up additional risk.

What happens is that these vendors who sell these systems to health care providers are reluctant to update the operating system with timely patching or antivirus protection, etc. And when the health care provider goes to the vendor and says, "I really need to update my equipment," the vendor will then respond, "Well, we can't do that because then we'd have to get recertified with the FDA," which is a common myth, the whole recertify by the FDA. It's not the true. The FDA has actually several times repeatedly denied that you have to do that. The standard maintenances would be covered and you wouldn't have to recertify.

However, vendors keep returning to that I'm sure as a way to save cost, and just a way to cut back on consulting expenses or support cost for providers. I think this particular rule is being put in place not only because of that, but because of HIPAA and HITECH and how PHI and EPHI (protected health information) is being transferred around the organization and riding on networks that are not just specific for health care or for medical devices. They're for the enterprise as a whole.

Peter: So the FDA is putting the onus on the medical practices. What sort of enforcement or teeth is built into this at this time?

Mike: At this time, there has been, based on my research and what I've discussed with other practitioners, there is no teeth that is listed as specific penalties. The FDA can, of course, inspect and, like the oversight they do with medical devices. Even though medical devices in particular are more stringent than medical device data systems, there are no particular teeth, which is similar to what happened in 1996 when HIPAA came on the scene. Lots of regulatory verbiage, lots of 'shalls' and 'wills', but at the very end of the regulations, there was no, "This is what will happen if you don't follow it."

It wasn't until very recently with the HITECH Act under the ARRA that significant penalties were placed on non-compliance, and also HIPAA got teeth with the HITECH Act. This may be a similar approach. This is the first shot over the bow to the medical device industry and also to health care providers, and they may follow up with additional regulatory compliance enforcement.

Peter: So as some work groups start to take a look at this stuff, then they'll probably have some responses. Just like HIPAA and HITECH, eventually there may be a little more enforcement with time.

Mike: I believe so. That's probably the trend.

Peter: Great. Mike, thanks very much. I appreciate it.

Mike: Thank you, sir. I appreciate it too.