**Podcast Transcript**

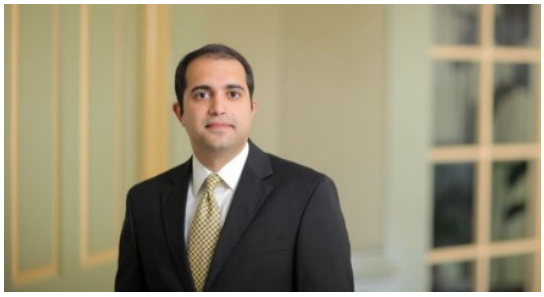
# Life Sciences: Connected Medical Devices in the Cloud During COVID-19

**Date:** August 3, 2020

**Guest:** Hussein Akhavannik, **Host:** Randall Rubenking

**Run Time:** 10:41

**For questions and comments contact:**




**Hussein Akhavannik**

Partner
Washington, D.C.
T: +1.202.861.1642 | hakhavannik@bakerlaw.com


Rubenking: Telehealth is having a big moment right now due to the COVID-19 pandemic. Telehealth has reduced strain on physicians and hospitals as well as safeguarded patients from potential exposure to infection. Not surprisingly, many medical device companies are looking to add or expand the remote monitoring capabilities of their devices. These capabilities however raise different legal issues that must be considered. I'm Randall Rubenking and you are listening to BakerHosts.

On today's episode we explore many of the legal aspects of connected medical devices with our guest Hussein Akhavannik. Hussein is a partner in the Intellectual Property Group at BakerHostetler and co-leader of the firm's Life Sciences industry team. He has a tech background in biomedical and computer engineering and focuses his practice on medical device and software prosecution. Welcome Hussein.

Akhavannik: Thank you Randall, it's great to be here.

Rubenking: Hussein, we know telehealth has been around for a while. Many people have smart watches and fitness monitors and the like, but with the pandemic it seems to have exploded. My smart watch already collects all my vitals. What other kind of devices are we talking about today and how do these connected devices help with patient monitoring?

Akhavannik: Smart watches and fitness monitors are definitely a big part of the telehealth universe, which is one reason why a lot of tech companies are investing heavily

in them. And while these wearables are collecting an increasing amount of information, such as your heartbeat, temperature, respiratory rate and physical movement, they cannot collect information from within the body. So, for example, if you're a diabetes patient your smartwatch cannot currently determine your glucose levels, or if you have a dermatology need, maybe take a picture of your skin to be able to send to your provider. They also don't know the type of treatment you're receiving. So, for example, the amount of insulin you're injecting, the times during the day in which you're doing the injection, or in the case of a pacemaker, when an electrical pulse is being applied to the heart. This information can be captured by the medical devices and other sensors in the body, or it can be entered by the patient using their phone. Then it's uploaded to a healthcare provider on a regular basis so that they can use that information to be able to update your treatment plan or adjust a treatment plan.

Rubenking: Okay. Well that's interesting, but why do I want another device to collect more information?

Akhavannik: Basically, it's providing you with better healthcare while saving you time and trips to the doctor's office. All this information allows your healthcare provider to monitor you in real time. And again, as we mentioned, to adjust that treatment plan as necessary. It also avoids these follow-up appointments we tend to have when there is a medical condition, which is especially important given the strain on our healthcare system. Over time that information that's being collected from you and other patients can be used to develop algorithms that predict an ailment even before you feel its symptoms. So, for example, a healthcare provider can alert you if you may have an ailment that you may not even feel symptoms for. There's an example right now in view of COVID where there's a wearable that can use your respiratory rate and temperature to predict if you have COVID even if you're asymptomatic, and a lot of sports leagues are now having their athletes wear them as they are either in the bubble or some of those sports that aren't considered in the bubble to be able to provide predictions.

Rubenking: I see. Okay, well now, what about patient's rights? The patient has to have some kind of data privacy rights as it concerns this health information, right?

Akhavannik: That's a really important concern for all of us. So, there are federal regulations regarding data privacy, specifically HIPAA, that requires consent when data includes health information that's associated with our identities. There are generally two types of entities that must comply with HIPAA when they're dealing with this information. One is obvious. It's what's called a covered entity, like a healthcare provider and insurance companies. The other one is not quite as obvious, and they're typically companies that are associated with those healthcare providers, such as pharmaceutical companies, medical device manufacturers and research centers. They are referred to legally as business associates of the covered entities. To gain access to the protected information, these business associates are required to execute a contract with the covered entities. These contracts have to describe the use of that personally identifiable information, state that the business associate will not disclose that information and explain all the appropriate safeguards to protect the data. However, there is

a carveout used for research. So basically, if the data does not identify any individual, then it can be used for research purposes without consent. And this kind of goes back to what we were talking about earlier where a lot of data is being collected from multiple patients. It can be aggregated and used for research purposes and that does not require consent of the patient.

Rubenking: Okay, very good. Now, I've read about hackers getting access to some of these things, like they can gain control of a pacemaker and other connected devices. What is being done to prevent this sort of thing?

Akhavannik: This is very scary especially in view of a pacemaker or another device that can sort of control life and death. There have been some research studies done that show that hackers, again in a research setting, can get access to different connected medical devices. And the FDA has been concerned about this for quite some time. The first cybersecurity guideline from the FDA was released in 2005 and most recently was updated in 2018, and the FDA has taken a very pragmatic approach. Basically, the security for different levels of risk is different. So, if you have what's classified as a tier one device, so a life-threatening device that's connected to the internet, so both can control life and death and also has the highest-level accessibility, because it is connected to the internet. There are certain requirements from the FDA for that type of device. Whereas a wearable, for example, that's connected via local network to your phone. Again, not life-threatening, just merely collecting vitals and a little bit tougher to hack into given its access that would have required a different level of security. So, what is the information that the medical device manufacturers have to provide the FDA? So the first is a description of the device itself. What risks are associated with the connectivity of that device? Testing done on the connectivity; so the wireless protocol, its encryption for example; and what the results of those tests were from a security perspective. And finally, all of these connected medical devices need to be labeled. The hazards and risks associated with the device have to be addressed. So, typically, not only is the information on the risks provided but also how those risks are being mitigated, including traceability and documentation.

Rubenking: Alright, Hussein. At the end of the day you're a patent guy. If a company has an existing medical device and then they add connectivity to it, how can they protect that aspect of their product?

Akhavannik: So, at a high level, to get a patent, your product has to be new and non-obvious. So, many think that adding communications to an already existing device would not clear that hurdle, but there are a few aspects you should consider when looking at your connected device. One, by adding communications hardware to the device you're gonna have to think about where that communications chip goes, so its positioning. If there is something kind of unique about its positioning, or a coding that you're providing if the device is in vitro. It might be in a harsh conditions in temperature or acidity, for example, that could potentially be patentable. The control of the communications hardware, first of all that communications hardware needs to be powered. Is it going to be drawing power from the existing medical device or from an external source? The communications itself, the data control, how is it being protected as we talked

about earlier, and how is it being transmitted to the phone or to a server if it's connected to the internet? If you're changing any aspect of the hardware on the existing device to add connectivity, that could also potentially be patentable. For example, there may be a single microprocessor on the device that's not gonna handle this added load of communication. What are the steps being done by that processor to manage that communication, for example? You may be adding a second processor to handle the communications to an already existing processor. Now that's gonna again, require power control placement on the circuit board itself, so I highly recommend that you talk to your patent lawyer about a very robust description of the changes that are being made to add connectivity to that existing device, because it may be patentable.

Rubenking: Hussein, we've covered a lot of information today. What would you like our listeners to take away from today's episode?

Akhavannik: I think everyone should understand that connectivity is increasingly important, especially in the new normal with restricted travel. The data captured by the connected medical devices is a new revenue source for companies that can used for drug development and treatment plans. So, the industry is moving toward connectivity, and this bears out in the patent filings in this space. These filings were almost nonexistent in 2000. They are now increasing in an exponential manner. Finally, know that your competitors are adding these features to their devices.

Rubenking: Excellent, thank you so much Hussein. If you have any questions for Hussein, his contact information is in our show notes. As always, thanks for listening to BakerHosts.