msk

ca iot law: devices at risk?

MSK Client Alert

March 26, 2019

In the last week, both the Dept. of Homeland Security and the Food and Drug Administration have issued a consumer alert about the potential hacking risk regarding cardiac devices, specifically because those devices have no encryption on their software. The devices in question are implantable cardiac devices, clinic programmers and home monitors which are used to regulate one's heartbeat rate – to speed it up or slow it down, as needed. The focus this time is on the Medtronic Conexus Radio Frequency Telemetry Protocol. Given this latest notice, one has to wonder what will be the impact of the California IoT law.

What both federal agencies had to say is short range access allows interference with, generation, modification or interception of communications. There is also the ability to read/write any valid memory location on the implanted device and, therefore, impact its intended functionality.

View Full Alert

attorneys

Susan Kohn Ross

practice areas

international trade

labor & employment

regulatory