COSMOS
Navigate the Compliance Universe

# Compliance Today - June 2019
# Ownership of healthcare data in the IoT era, Part 1

By Robin Singh Ms(Law), MBA, Ms(IT), CCEP-I, CFE, HCCP

**Robin Singh** (robin@whitecollar.org) is Compliance and Fraud Control Lead Officer at Abu Dhabi Health Services Company (SEHA) in the United Arab Emirates.

**This is the first part of a three-part series that will focus on the how the world of the Internet of Things (IoT) works, its variabilities, and privacy concerns when it comes to a healthcare system.**

The Internet of Things (IoT) is still something that most of us are trying to wrap our heads around, and the very term itself isn't exactly helping the cause. However, for the sake of convenience, let's define it as an era of connected devices that will soon envelop the future we are heading towards. But, connected devices aren't a new thing. We've actually had them for a while. For instance, on-board diagnostic units (OBD) that keep drivers informed have been in vehicles for a few years now.

But, as usual, technology rarely remains stagnant and things keep changing. Today, the deployment architecture has evolved significantly. With new standards and more addressability, we are finally entering a time when having every device connected to the other has become a reality. Cisco projects that 50 billion devices will be connected to the Internet by 2020,[1] and Strategy Analytics forecasts that the IoT market will be worth $242 billion in 2022.[2]

Now, irrespective of how grand that might sound, it is always good to possess a healthy dose of skepticism about these things. Technology has never been without challenges, and the IoT is a new frontier that still remains unexplored. The biggest and most apparent challenge thrown in by IoT is the challenge of data ownership and privacy. The key question is: Who owns and controls the data? Is it you? Is it the service provider, manufacturer, or vendor?