COSMOS
Navigate the Compliance Universe

Compliance Today - July 2019

Ownership of healthcare data in the IoT era, Part 2

By Robin Singh

Robin Singh (robin@whitecollar.org) is Regulatory Compliance and Fraud Control Lead at an Abu Dhabi healthcare government entity in the United Arab Emirates.

***This is the second in a three-part series that will focus on how the world of the Internet of Things works, its variabilities, and privacy concerns when it comes to a healthcare system. Part 1 was published in the June 2019 issue of* Compliance Today.**

To predict what data ownership and control might look like in the Internet of Things (IoT) era, we must first understand how everything works now. Essentially, machine-generated data (MGD), which is what we'll be seeing more of in the IoT era, is owned by the entity that owns the device that collected or recorded the data in the first place. In other words, if you're the owner of a smart device, the data recorded on it is yours.[1]

How data ownership currently works

But, that's only true if you see it from the perspective of a social contract. In the real world, where "imagined agreements" do not enjoy any validity, things get complex and murky. Of course, most of us understand that only the device owner can claim ownership over data. Here, data isn't very different from, let's say, a property deed.

But, it is possible for data to be owned by one entity and controlled by another. Possession doesn't always translate to legal ownership. So, for all practical purposes, we have what is known as usage rights. So, all the data that's generated by your device is copied, transmitted, and controlled by the manufacturer, service provider, etc.

You see, there are no actual protections offered in terms of data ownership under American intellectual property laws. However, we do have data title rights, which are similar to the protections offered by the copyright law. In the European Union, an entity that collects a lot of data will be governed by the General Data Protection Regulations (GDPR). Regulations such as GDPR and the California Consumer Protection Act (CCPR) will help target a focused result set, giving regulators and security consultants a level playing field. Regulators can be successful in their implementation as long as people are alert and can believe that their role is equally important in protecting their own privacy rather than being dependent. Remember, make an informed decision to claim "my privacy my right" (#myprivacymyright). Provisions such as the "right to be forgotten" provision in the GDPR will be tough to implement, because the user/consumer will not know where to go for help or whom to approach.

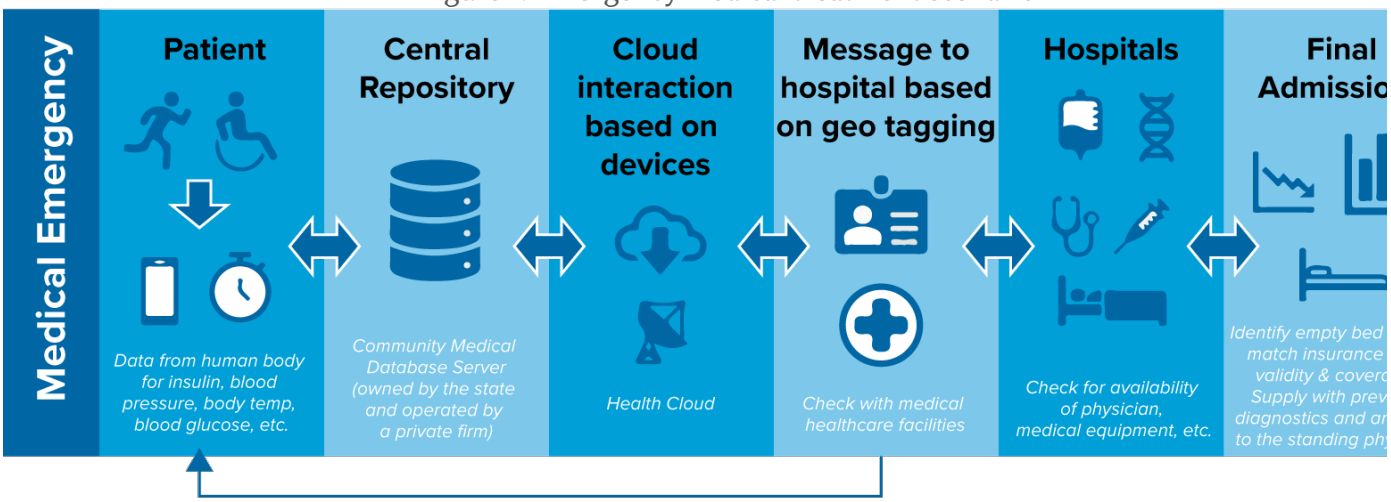
Data title rights are rights that allow the data owner (titleholder) to do as they please with their data. This means they can copy, distribute, and even develop derivative works based on it. The data here refers to any content such as an image or a video. Think of it like the letters and pictures that make up a book. The book here is the database and, like a book, it's got title rights but no usage rights. In other words, you own the database and the data, but if you choose to put it all out there, you have no rights over how it is used.

Remember when you started a new app and either the Android or Apple device asked you for permission to use that, and use this, and you clicked OK on most of them without properly reading the agreement? That's the first generic level to access demanded by most of the companies using your data.

A myriad of third parties are involved and raising hands to share and take care of data and disseminate your data

to multiple stakeholders that take care of various aspects of IoT. Figure 1 illustrates the situation that a normal patient would be faced with in case of an emergency.

Figure 1: Emergency medical treatment scenario



A human body is the source of big data. Patients with unique conditions are an even bigger source of data for providers and hospitals. Providers tend to sell solutions, even for conditions which they might not specialize in. If they can get the patient to buy into their vision of recovery, they can gain access to that body, and thus the source of big data.