Why Things Matter

by Barry P. Chaiken, MD, MPH

Compared to automobiles made just a few years ago, new ones provide an amazing driving experience. Expanding beyond the CD changer and iPod® dongle, automobiles now integrate our smartphones and use voice recognition technology, allowing drivers to keep their hands on the steering wheel.

In addition to this high-tech experience, automobiles contain electronic black boxes that collect data from numerous sensors implanted throughout the car. These devices monitor acceleration, speed, braking, engine performance, turning radius, and other parameters. Automobile manufacturers access the data in the black boxes when the cars return to the dealer for service and aggregate it to better understand how well their cars perform under real-world driving conditions. The huge amount of data allows for stratification of drivers into different driving categories. Combining this valuable information with owner demographics, manufacturers have leverage that can inform car design, safety improvements, and targeted marketing.

Automobile insurance companies and law enforcement see value in this data for accident investigations and as a source of criminal evidence. In the near future, our insurance rates may be set by how we drive, as indicated through the data collected by our cars, rather than the types or number of actual accidents. Will we all drive under the speed limit, knowing that our cars are monitoring our behavior and the data being collected could be used to raise our premiums?

Sensors provide the foundation for the Internet of Things (IoT) technology movement. The precipitous drop in the cost of manufacturing computer chips, and, in turn, sensors built upon those chips, allows the production of cheap, disposable devices. In addition, a new Internet addressing protocol—IPv6—provides a means to assign a unique address to every sensor. Wikipedia defines IoT as:

> *The network of physical objects—devices, vehicles, buildings and other items—embedded with electronics, software, sensors, and network connectivity that enables these objects to collect and exchange data. (Internet of Things, 2016)*

Creating sensors with unique Internet addresses allows them to be controlled across the existing Internet infrastructure. This integrates the devices into the physical world, providing valuable insight without the cost associated with direct observation. In addition, the sensors can be designed to collect data that permit the intelligent management of a particular process, service, or activity.

Medical IoT

Using sensors and other IoT devices to monitor and manage patients offers clinicians information that was previously unavailable. The traditional collection of patient data in an episodic manner—each time the patient visits the provider—pales in comparison to collecting patient data in any setting, at any time. In addition, the data collected include measures formerly unavailable or cumbersome to aggregate.

Each of these data points—temperature, blood pressure, activity level, and gait, for example—can now be collected with minimal intrusion on a patient's lifestyle or activity. When coupled with therapeutic protocols, medical IoT devices allow for closer monitoring and improved management of patients, particularly those with chronic disease. Here are some examples of how medical IoT can be utilized:

Medication compliance. Problems arise when patients do not complete their prescribed antibiotic regimen. In addition to increasing the likelihood of a failed treatment, an incomplete regimen encourages the development of drug-resistant infectious agents. Medical IoT devices linked to prescription bottles, or even to the pill itself, can monitor the consumption of the antibiotic, alert patients to take their medications, and notify clinicians of noncompliance.

Remote monitoring. Many patients with chronic diseases require close monitoring. For example, changes in the activity levels of elderly patients with heart disease provide a first indication of a worsening condition. Sensors can be used to monitor activity and alert clinicians to the need for intervention.

Clinical trials. Data collection forms the bulk of the costs of randomized clinical trials. Each measure collected adds increasing complexity and cost to the research. In addition, inaccurate or incomplete data collection heightens the risk of a failed trial. The closer the trial adheres to its actual design, the better and more valuable the research results. Medical IoT increases the number of data points that can be collected, raises the likelihood of collection, and reduces the cost of aggregating the data.

Many more applications of medical IoT are focused on better surveillance and clinical management of patients. In addition, medical IoT offers patients the ability to self-monitor conditions and adjust treatment as instructed and needed.

Not free of risks

Although medical IoT offers great benefits, it also presents several challenges and risks. Many security threats

on the Internet, such as viruses and ransomware, present an environment where sensor-generated data could be harvested and used for criminal purposes. Similar to theft of financial information, the sensor data can be used to steal identities, impersonate individuals, or extort money from victims. Therefore, hardened security protocols and technology are required to protect patients.

Similar to anecdotal reports of cars being "attacked" by hackers, devices controlled by medical IoT are at risk. Any deployment of these devices demands a robust plan to prevent their infiltration by hackers who may be inclined to injure patients, or to lash out at the manufacturers of the sensors or the provider organization using them.

As the medical IoT market evolves, the FDA must remain current with new technologies and, in turn, determine the level of oversight required. The FDA will balance potential risks to patients with the need to encourage innovation. As these sensor technologies and supporting software evolve rapidly, the FDA will need to access adequate expertise to make proper determinations. This will not be an easy task.

Finally, medical IoT opens up an area of medical liability that remains undefined. If sensors fail and there is an unexpected event, is the sensor manufacturer or the provider responsible? What level of harm must be present to trigger liability?

Despite all the challenges posed by medical IoT, the benefits far exceed the risks. Allowing providers to monitor their patients more closely delivers better outcomes. Giving patients access to more information about their conditions affords them better control over their treatment. Medical IoT presents an unlimited number of possibilities to improve clinical and financial outcomes. The sooner visionary innovators create the use cases and the sensors, the better.

Barry Chaiken *is the president of DocsNetwork Ltd. and has more than 25 years of experience in medical research, epidemiology, clinical information technology, and patient safety. He is board certified in general preventive medicine and public health and is a fellow, and former board member and chair of HIMSS. At DocsNetwork, Chaiken worked on quality improvement studies, health IT clinical transformation projects, and clinical investigations for the National Institutes of Health, UK National Health Service, and Boston University Medical School. He is currently an adjunct professor of informatics at Boston University's School of Management. Chaiken may be contacted at bchaiken@docsnetwork.com.*

REFERENCE

Internet of Things. (2016, May 9). In *Wikipedia, The Free Encyclopedia.* Retrieved May 10, 2016, from https://en.wikipedia.org/w/index.php?title=Internet_of_Things&oldid=719442160