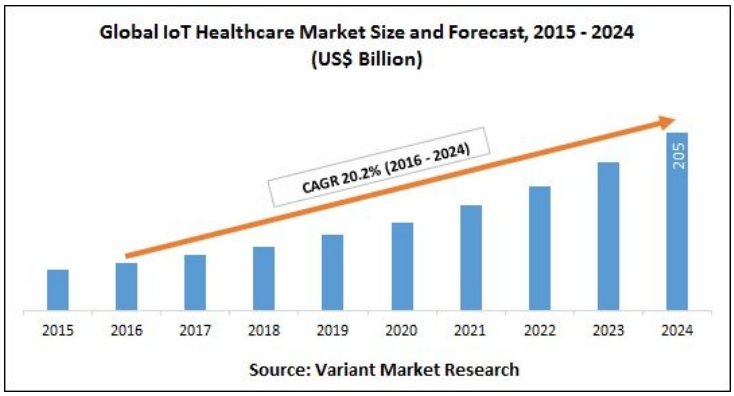
BioSpectrum
the business of Bio & Health Sciences
ASIA EDITION

IoT connected medical devices promise a better tomorrow

February 8, 2018 | Analysis | By Aishwarya Venkatesh

IoT connected medical devices is poised to revolutionize the functioning of the healthcare industry. While there are many benefits of the IoT connected medical devices, it comes with its own challenges



2018 is here and it is no doubt going to be the year of innovations and technology. FDA closed 2017 on a positive note by granting approval for Alive Cor's Kardia band, a real-time electrocardiogram (ECG/EKG) housed in a watch strap. Yes, you heard it right! ECG in a watch strap! AliveCor already sells an FDA-approved device called Kardia Mobile, a strip attached to the back of a smartphone. The device requires the user to place two fingers of each hand on the strip for a 30-second reading. However, this newly approved Kardia band device is more discreet and extends the technology into continuous rather than on-demand monitoring. It detects normal sinus heart rhythms and atrial fibrillation (AF), the most common heart arrhythmia.

"Several times when I was in atrial fibrillation, I was able to talk with my doctor by phone and adjust medication and avoid a trip to the ER. As they say, knowledge is power; in my case, knowledge leads to peace of mind." reads a testimony in Alive Cor website.

Rewind back to 100 years ago, when the first ECG's were invented, they were huge machines, took upconsiderable space and often required patients to submerge their limbs in jars of salt solution. A century later, ECG equipment has advanced to the point that it can be integrated into a smartwatch that's capable of far more. AliveCor, the watch band's creator, is alive to the healthcare opportunities that come with technological advancements in medical devices space.

Atrial fibrillation (AF) is the most common heart arrhythmia and a leading cause of strokes, affecting over 30 million people worldwide. Many people are unknowingly living with AF, yet two out of three strokes are preventable when AF is detected and treated. There is therefore huge scope for accessible real-time monitoring solutions to help prevent major heart-related health issues. With an ECG device on the wrist, AF can be detected wherever the patient is, 24 hours a day.

Thus, preventative measures that utilize IoT in healthcare not only stand to benefit the patient, they also go a long way to lowering costs for healthcare services and expensive treatments. Now next generation medical devices are the in-thing. By harnessing the power of technology, device manufacturers are connecting devices to the IoT, using additive manufacturing (3D printing), producing wearable electronics ("smart" clothing, skin-adhered sensors) making remote and continuous monitoring of a patient's health possible.

IoT enabled medical devices is the way forward.

It was only 25 years ago that the web really started to take off. Now everyone is connected and soon "everything" will also be connected through internet of things (IoT). Imagine a scenario sitting at the comforts of your home and getting a dialysis done! No hassles, no visiting doctor facilities, patient can get his dialysis done with the help of a portable/home machine designed for the purpose. Data gathered from this device is analyzed and stored, and helps make informed decisions in a timely manner. Caregivers can monitor the patient from any location and respond appropriately, based on the alert received. Advanced treatment of this nature harnessing IoT can drastically improve a patient's quality of life.

The IoT has myriad applications in healthcare that benefit patients, families and physicians alike. Around 20 billion devices are expected to be connected to the internet in the next few years, experts say. The global Internet of Things (IoT) in healthcare market is forecasted to reach $410 billion by 2022, according to a Grand View Research report. Health and wellness is one of the most promising application areas of IoT technology. Remote health management, managing lifestyle-related diseases and conditions, fitness programs, care at home, chronic diseases and care for the elderly are some of the important use cases. Medical devices such as personal home-use diagnostic devices or low-end diagnostic and imaging devices that are used by mobile health workers are one of the key technology components.

Hence, for device companies to succeed, in this highly competitive market, it is important that they think beyond traditional practices and integrate technology into their products. The demand for devices with integrated sensors, controllers, wireless connectivity, firmware and remote monitoring is being fueled by several healthcare trends. These include transitioning of care delivery from acute settings to the community; increased patient interest in tracking their own health; rise in economic status and disposable income; an aging population with chronic conditions with greater focus on preventive healthcare to drive down costs. A connected healthcare environment promotes quick flow of information and enables easy access to it, improves home care facilities and provides regular health updates to clinicians. Connected health solutions can also be used to track lifestyle diseases such as hypertension, diabetics and asthma which need continuous monitoring. All these factors have created strong incentives for designing devices built on the latest technology and getting them to market faster than the competition.

But healthcare IoT isn't without its obstacles.

Recently hacked medical devices are making scary headlines! The number of connected devices and the tremendous amount of data they collect can be a challenge for cybersecurity. Last year, the FDA took the unprecedented step of recalling 4,50,000 pacemakers because it was found to be vulnerable to cyber threats. Johnson & Johnson, last year, had warned customers about a security bug in one of its insulin pumps. It is important to excise security and protect patients, so that attackers don't hack an insulin pump and administer a fatal dose. Medical devices also connect to a huge array of sensors and monitors, making them potential entry points to larger hospital networks.

Implanted devices are so personal and nobody will want something in your body to be remote controlled by a hacker. A recent study by Synopsys highlights that only 51 percent of device makers and 44 percent of healthcare organizations follow current FDA guidance to mitigate or reduce inherent security risks in medical devices. Fortunately, medical device vulnerabilities have been on the FDA's radar for some time. In July 2015, the FDA issued an Alert highlighting cyber risks related to infusion pumps. Then, at the end of 2016, it issued what it called "guidance" on the post-market management of cybersecurity for medical devices.

FDA in its website, says, "All medical devices carry a certain amount of risk. The FDA allows devices to be marketed when there is a reasonable assurance that the benefits to patients outweigh the risks. While the increased use of wireless technology and software in medical devices also increases the risks of potential cybersecurity threats, these same features also improve health care and increase the ability of health care providers to treat patients."

Thus, IoT connected medical devices is drastically change the face of healthcare monitoring, treatment outcomes thus promoting a better standard of living. Nations across the world are struggling to improve patient care and these connected devices provides a timely and cost-effective response to this critical imperative. Moreover, recent developments in sensor, internet, cloud, mobility and big data technologies have led to affordable medical devices and connected health programs, vastly increasing the potential of IoT enabled medical devices to influence further changes. However, connected devices are vulnerable to security breaches and statistics reveal that that manufacturers are not building these devices with security as a priority. As IoT devices grow in popularity, seemingly endless security- and privacy-related concerns are surfacing and need to be addressed.