



How IoT Is Transforming The Future of Healthcare

WHITE PAPER

According to a report released by National Institutes of Health in 2016, the world's older population is growing dramatically. 8.5% of people worldwide (617 million) are aged 65 and over and this is projected to jump to nearly 17% of the world's population by 2050 (1.6 billion). To add on, global life expectancy at birth is projected to increase by almost eight years, climbing from 68.6 years in 2015 to 76.2 years in 2050¹. Together with the rise of chronic illness, this will, if it hasn't already, increase the demand in healthcare and push the current systems beyond its limit and capabilities. Hospital staffs will be asked to do much more than what they can handle. To make matters worse, societies have rising expectations for more and better health services. Hospitals and healthcare facilities will face difficult times balancing expectations against available resources.

Technology – Advancing Healthcare

Fortunately, technology is here to provide some form of change to the medical landscape in a dramatic way. Wireless devices are not new, but they have been integrated more and more into the hospital environment, improving healthcare services. These wireless medical devices help healthcare providers improve real-time patient status and respond promptly to critical patient data. With increasing numbers of wireless medical devices, hospital staffs are able to monitor patients' health remotely without being physically present, making it possible to care for more patients.

Internet of Things (IoT), or to be more specific, Internet of Medical Things (IoMT) or Healthcare IoT is defined as the collection of medical devices and applications that connect to healthcare IT systems through online computer networks. A FitBit is a simple example of an IoMT device; someone that wears a FitBit can track his or her steps and that information will be linked to a smartphone or tablet via Bluetooth technology. This collection of data will then be sent to the patient's physician or close family members for feedback, via Wi-Fi connection. Another more life-critical example would be pacemaker; a pacemaker is a small device that is placed in the patient's chest or abdomen to help control abnormal heart rhythms. This device uses low-energy electrical pulses to prompt the heart to beat at a normal rate. When a patient's heart rhythm is abnormal, the computer will direct the generator to send electrical pulses to the heart. Highly programmed pacemakers have been responsible for reducing patients' risk of death, hospitalization for heart disease and permanent irregular heartbeat by 26%².

IoMT is revolutionizing the healthcare industry. Doctors are now able to better diagnose and treat patients, prescribe targeted and personalized medicine, as well as improve communication and workflow for hospital staffs. These are considered as basic necessity today, but there are demands for greater technological advancement and that is why healthcare IoT is establishing itself in the modern everyday living.



IoMT is revolutionizing the healthcare industry. Doctors are now able to better diagnose and treat patients, prescribe targeted and personalized medicine, as well as improve communication and workflow for hospital staffs



The Changing Landscape of Healthcare IoT

The number of connected medical devices is expected to increase from 10 billion to 50 billion over the next decade³. These interconnected devices will be generating continuous data, stored either in the healthcare facility or in the cloud. Cisco estimates that by the year 2021, the total amount of data created (and not necessarily stored) by any IoT device will reach 847 ZB per year⁴. At some point, IoT will become the biggest source of data on the planet. Imagine the possibilities if human-oriented data, like medical history, medication and allergies, laboratory test results, personal statistics and age, amongst many other things, were to be digitized as part of the electronic health initiatives. Healthcare practitioners will be able to understand and leverage the plethora of big data from connected systems to make more informed care decisions as well as understand and predict current and future health trends. The answer? Machine Learning (ML).

Machine Learning Helping To Propel Healthcare IoT

ML is an approach to achieve artificial intelligence (AI) - the practice of using algorithms to analyze data, learn from it, and then make a decision or prediction about something in the world. Healthcare providers and device makers are integrating AI and IoT to create advanced medical applications and devices that can provide person-centric care for individuals from initial diagnosis to ongoing treatment options, while solving a variety of problems for patients, hospitals and the healthcare industry. At the same time, these AI-enabled medical IoT devices will make healthcare treatments more reactive rather than preventive.

Here's an example of AI-enabled medical IoT application – an autonomous 'nurse' that can be connected to the internet or cloud and to a large range of data from previous health records and other personal information. A robotic 'nurse' will be able to answer patients' questions with the freshest news or data that it has. By integrating facial recognition, the robotic 'nurse' will be able to recognize a patient's mood and will adapt its behavior and reaction accordingly. It will also be able to remind its patients to take medication accordingly, as well as remind them of their doctor's appointments. Now, imagine if a hospital were to 'hire' robotic 'nurses' that are able to reason, make choices, learn, communicate, move and are connected to the hospital's network and connected to each other. They would be able to help the nurses with tasks like administering medication, maintaining records and communicating with doctors and educating patients and on disease management, just to name a few. This will be a solution to alleviate the situation where the nurses sometimes are pushed to handle more than they are capable of.



At some point, IoT will become the biggest source of data on the planet. Healthcare practitioners will be able to understand and leverage the plethora of big data from connected systems to make more informed care decisions as well as understand and predict current and future health trends.



Machine learning will help to transform the way patients are being diagnosed and treated in the hospitals, and healthcare professionals provide a better quality of care that is tailored to each patient based on their sensor readings and analysis.

AI is gaining a lot of traction in healthcare IoT space. According to an analysis done by Accenture, key clinical health AI applications can potentially create \$150 billion in annual savings for the US healthcare economy by 2026⁵. This includes integrating applications like robot-assisted surgery, virtual nursing assistants and administrative workflow assistance into the healthcare industry.

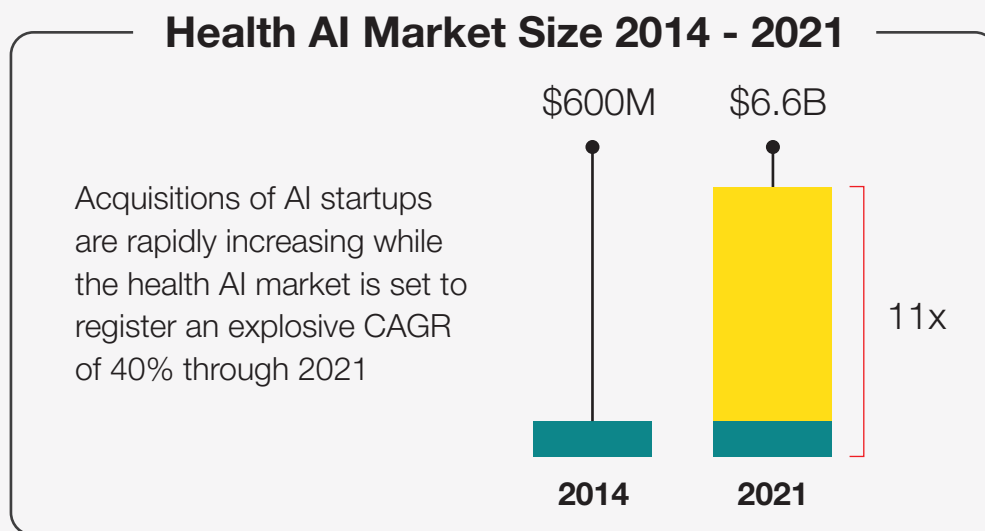


Figure 1. The AI health market is seeing explosive growth.”

Not only will ML bring a set of bots to the healthcare industry in the near future, with billions of ‘dumb’ machines being transformed into smart machines, it is going to transform the way patients are being diagnosed and treated in the hospitals, and healthcare professionals provide a better quality of care that is tailored to each patient based on their sensor readings and analysis.

^{**} https://www.accenture.com/t20171215T032059Z__w__/us-en/_acnmedia/PDF-49/Accenture-Health-Artificial-Intelligence.pdf#zoom=50

Medical Drones To The Rescue

There is also a new application where drones are used to deliver medical supplies, especially to rural areas where one will find small under-equipped medical facilities. In a recent report⁶, drones, also called the “Flying IoT” have started to deliver medical supplies like red blood cells, plasma and platelets on a life-threatening event in Rwanda. The rapid delivery of critical supplies by drones would save lives when patients cannot be transported to healthcare facilities quickly by ambulance or helicopter.



There are many activities around drones today; many companies are starting to develop drone systems to transport medical supplies, researchers are working on solving refrigeration issues when storing blood packages, and efforts to make drones more energy efficient so that it will move faster. There is no doubt that the usage of drones in healthcare industry is getting a lot of attention and is slowly scaling up in countries like the United States, Switzerland and Australia. It is only a matter of time before the drones are universally adopted for emergency and disaster response toolkits.

A bright Future For Telehealth

Another new development that the healthcare industry is seeing today is a general shift from hospital care environment to private care environment like remote health monitoring or telehealth. Many would agree that the home is the best place for healthcare, with patients being in their ‘normal everyday environment’. A survey conducted in 2016 concluded that 94% to 99% of 3,000 patients were very satisfied with telehealth, while one-third of the respondents preferred the telehealth experience to an in-office doctor visit⁷.

With IoT, remote health monitoring, or telehealth is possible. It can help to solve chronic diseases, even for patients who live in remote areas. Another reason why remote health monitoring is gaining popularity is because of the vast varieties of biosensors and medical wearables that are available readily in the market today. So, what’s in it for the healthcare practitioners? All these data collected from remote patients can be analyzed to detect patterns and gain new insights into health trends. That’s what IoT, big data and analytics software can help to achieve.

Challenges Ahead

With all the technological advancements that we are seeing today, the Internet of Medical Things (IoMT) industry is still thriving and its landscape is still changing. The shift in demographic, digital transformation, influence from the government as well as consumers' demand for value-based care are just some of the trends that is causing this change. While these changes are taking shape, there are ample of challenges that needs to be addressed - information security, interoperability and regulatory, among many others.

The Vulnerable State Of Healthcare Data

Healthcare cybersecurity is a growing concern. There have been several large security breaches and hacking cases seen over the last few years and many healthcare organizations have struggled to defend and keep the cybercriminals off. A prime example is the 2015 Anthem/Blue Cross security breach, that resulted in the loss of personal identifiable information (PII) of 78.8 million people⁸ – one of the biggest data breaches of the 21st century. A report has shown that 41% of IoT related security incidents in the healthcare industry were caused by bad user practice. Outdated OSES and software account for another 33% of the IoT security related incidents⁹. The WannaCry ransomware attack in May 2017 was a good example of how the continued use of outdated software and failure to patch vulnerabilities promptly can cause cybersecurity issues.

With the sheer volume of health data created from billions of connected medical devices, securing the device, and ultimately the data, is a responsibility that needs to be acknowledged by all parties – governmental healthcare organizations, device makers, hospital administrative and healthcare practitioners. FDA has taken a step to develop a five-point action plan that requires medical device makers to incorporate capability to update their devices throughout the entire life cycle of the products. Healthcare administrative and healthcare practitioners should acknowledge the fact that the cybersecurity threat is real and without strong security measures, they are putting themselves and their patients at risk. To help alleviate the problem, they should also take steps to improve their network securities and protect their hospital, following a set of comprehensively defined security practices.



With the sheer volume of health data created from billions of connected medical devices, securing the device, and ultimately the data, is a responsibility that needs to be acknowledged by all parties – governmental healthcare organizations, device makers, hospital administrative and healthcare practitioners.

Interoperability – Critical To Drive Successful IoMT

Medical device interoperability concerns are rising along with the increase of connected medical devices in a healthcare facility. It is also one of the reasons why some healthcare facilities are not realizing the benefits of connected healthcare today. Medical devices, technologies and systems that are interoperable should be able to effectively exchange information with each other and EHRs, to display, interpret, analyze and automatically act on or control other devices, in a consistent, predictable and reliable way. Lack of interoperability creates significant sources of waste and risk to patient safety, due to the fact that healthcare practitioners will need to depend on incomplete or stale information for workflow or decision making.

Over the years, interoperability has shot to the top of the healthcare industry's action list and a wide variety of healthcare organizations including regulators, healthcare providers and consultants have come together to form the international standards development organizations (SDOs), to develop standards for worldwide adoption. Some of the major SDOs involved in the development of interoperability standards to facilitate the exchange of health information are, International Standards Organization (ISO), which collaborates with European Committee of Standardization (CEN) and Health Level Seven (HL7), and has a membership of over 20 participating countries. OpenEHR and Integrating the Healthcare Enterprise (IHE) are two other SDOs that are heavily involved in developing standards, focusing on EHR and computer systems respectively. It might seem like many standards have been developed and adopted globally, but steps have been taken to regulate and converge them to achieve true interoperability.



Standards And Regulatory Hurdles

With all the exciting technological development happening in healthcare IoT, it is unavoidable that there will be some new uncertainties. For example, in the midst of analyzing the data to create new insights and providing new services to patients, the connected medical devices that shares information through clouds might expose patients' data to hackers who can infiltrate the wireless networks that connect the medical devices. There needs to be some form of regulation to govern the healthcare IoT, from the perspective of patient protection, especially as it relates to security and privacy.

In order for healthcare IoT to grow across the horizon, governments cannot operate in silos. Today, governments are addressing cybersecurity and networked medical devices via new regulations separately. As an example, in the United States, HIPAA regulations, particularly the security rule, outlines the need to protect Electronic Protected Health Information (ePHI) that is created, received, used and maintained by doctors, pharmacies, health insurance companies or any vendor that is in contact with patient data. Apart from that, there may be additional regulations from the FDA (Food and Drug Administration), FCC (Federal Communication Commission), and FTC (Federal Trade Commission), among others, all in the effort to secure the healthcare IoT industry. Europe, on the other hand, has the General Data Protection Regulation (GDPR) to address the threats that is posed by IoT. GDPR requires companies to state up-front what type of data will be gathered and how it will be used. Countries like United Kingdom, Japan, Russia and China also have administered different sets of regulations.

Today's situation is not ideal. There is no single regulatory body that could manage an area as vast and complex as IoT. However, despite the dangers of lack of uniformity in terms of regulation around privacy, hopefully the differences will call for some reflections and eventually learnings to help balance the interests of innovation with patient protection.



Forging Ahead

IoT is a game-changer. Digital transformation is rapidly transforming the healthcare industry. Healthcare practitioners can do away with manual data entry, be more efficient and avoid the risk of errors in data entry. They will be able to focus their time and effort on more clinical cases. Patients are undergoing the transition from passive recipient of healthcare to active value-seeking consumers. A system-wide improvement in quality of care is achieved through simplified clinical work-flow, and the number of steps to diagnose and treat a patient is reduced. With digital transformation forging ahead along with new government regulations, healthcare providers will need to adopt a variety of applications that are interoperable, coupled with straightforward access to their IT infrastructure to drive the healthcare industry's critical need for service assurance, now and in the future.

For more information about how Keysight Technologies and Ixia, a Keysight Business, is able to help in the transformation of Healthcare IoT, go to www.keysight.com/find/healthcareiot

References

1. International Population Reports - An Aging World
2. MedicineNet.com Newsletter
3. MedicalDesign and Outsourcing
4. Cisco Global Cloud Index
5. AI:Healthcares New Nervous System
6. Fast Company: World Changing Ideas
7. First Stop Health - Telemedicine News
8. Wikipedia - Anthem medical data breach
9. TechRepublic - Internet of Things Newsletter

Learn more at: www.keysight.com

For more information on Keysight Technologies' products, applications or services, please contact your local Keysight office. The complete list is available at: www.keysight.com/find/contactus

