The Leading Edge of Disruptive Innovations in Health Care Data, Communications, and Information Technologies:

Internet of Medical Things

A 2019 Primer and Perspective

Gregory Downing, D.O., Ph.D.

Produced for the Global Digital Health Partnership, 2019

NOT FOR DISTRIBUTION

The issues and views discussed herein are for discussion purposes only and not reflective on the Global Digital Health Partnership perspectives or policies.

ABSTRACT

This issue brief explores the topic of the Internet of Things (IoT) and the basis for its current surge in applications across the health care sector. Here, we explore IoT, specifically for medical applications, from a historical perspective, terms and definitions, the major science and technology components, and, relevant to the Global Digital Health Partnership (GDHP). The technical advances of data exchange among machines and human-machine interfaces has opened a wide field of innovation for integrating data from sensors, medical devices, smart phones and other platforms for data capture. The features of multi-functionality, low cost, mobile, and widely adaptable sensing and emitting characteristics of IoT devices has created opportunities for efficient and rapid collection and exchange of data. The intention behind this document is to provide a general view on the fundamentals of IoT functionality, its current and future applications, and an overview of the dominant issues about it that government organizations are engaged in. Of particular interest, the importance of cybersecurity provisions and privacy protections pertaining to IoT applied to personal and institutional data are paramount. As a result of the basic understanding presented here, coupled with unique perspectives and experiences of each of the individuals in the audience, we encourage thoughtful exploration of the role of government in shaping the future of role of IoT in health care by the GDHP community.

01 Internet of Medical Things

1.1 Objectives in Our Understanding of Data and Communications in Health Care

Across the world, the applications of communication and information technologies are a major area of advancement in applying access to, and use of, medical care. Whether it is in consumer or personal health needs, public health applications, long-term care, or acute care settings, the advantage of rapid, mobile interconnectivity is a landmark of technology advances across all of health care and society. The revolution that digital communications provide in distance learning, support of autonomous functions, and augmenting intricate and highly precise human functions has opened the door for rapid expansion of interconnectivity among devices that can perform at dramatic speeds with high fidelity and low costs. The “Internet of Medical Things” (IoMT) enables machine to machine interaction and real-time intervention solutions which has quickly become a radically transformative set of platforms to disrupt healthcare delivery and enhance affordability and reliability of health care services in near future. Additionally, IoMT provides a new social plane of interactive human interaction that can serve to increase patient, provider and caregiver engagement in decision making. As individual humans grant authority to machines to share data, IoMT will overcome barriers to interpersonal exchange resulting in better understanding of complex care medical issues and improve outcomes of health care services.

By providing the individual data driven treatment regimen and optimized devices to meet the medical requirement for standards of practice, IoMT will promote personalized care and high standard of care in more diverse communities and settings to overcome access barriers. Moreover, recent engineering research and development in sensors, networks, cloud, mobility and big data domains, will continue to open new doors of opportunity for remote care with affordable medical devices yielding a more connected health ecosystem.

The uses of IoT in all aspects of personal, commercial and societal domains of technology are expansive and rapidly growing in their implications. This white paper provides some key understandings of this technology with a focus on health care and medical capabilities that are enabled through these features and will be referred to here as the Internet of Medical Things (IoMT). Here were provide an overview, analysis, and insights into the future of IoMT with a focus on the impact on health and healthcare that can be anticipated in the next 5 years.

1.2 What is IoT?

To fully grasp the future contextual applications of data and devices that are connected, it is helpful to understand some of the basic features of IoT. Basically, IoT is the concept of connecting any device with a digital switch to the Internet and, therefore, connecting these devices to each other. This includes anything with digital communications such as mobile phones, electronic appliances, medical devices, personal computers, industrial machines including automobiles, airplanes, and trains. The result of these digital connections, currently estimated by Gartner to be 26 billion connected devices as an incredibly large “internet-of-things” by 2020.[i] As a result, this network has enabled between people and things in vastly new ways and unforeseen scale of connectivity.

The term came into common use early in the 21st century, but the actual idea of a network of connected devices was often called “embedded internet” or “pervasive computing” in early engineering and business literature. The actual term “internet of things” was coined by Kevin Ashton in 1999 during his work at Procter & Gamble. Ashton who was working in supply chain optimization, sought to attract senior management’s attention to a new technology platform called radiofrequency identification (RFID).[ii] Because the internet was a burning new platform for business in 1999 and because it somehow made sense, he called his presentation “Internet of Things.”

1.3 Why IoT?

The Internet of Things ecosystem has a very complex architecture, in which multiple components interact with each other to enable various solutions for the end user. This is an interdependent system, which enables real-time data acquisition, device connectivity, data transfers, and analytics to control end user applications. IoT provides the connected environment, comprising the cyber physical systems, which integrates human intervention with computer-based systems and facilitates data-driven decision processes. Currently, IoT encompasses technologies such as smart grids, smart homes, intelligent logistics, and smart towns, augmented through sensor, actuator, and communication protocol networks. IoT offers various real-time solutions through the integration of data analytics and sensors embedded on machines.

1.4 Health Care Services and Applications of IoMT

In addition to other industry segments sectors such as manufacturing, construction, and power distribution, healthcare is poised for a transformation through IoT. Healthcare application of the IoT technology, comprises a network of connected devices that sense vital data in real time. IoMT can refer to a wide variety of devices such as heart monitoring implants, infusion pumps that are used in hospitals to deliver a pre-programmed level of fluids into a patient. There are also millions of other devices like pacemakers, insulin pumps, and cochlear implants. Some of these devices only send information via a wireless connection like a pace maker, while others can send and receive information. There are also devices know as wearables, like the Apple watch or the Fitbit, that can track vital information including your daily activity information, including the number of steps taken or calories burned. At some point this data is synchronized with the personal watch or another device, including electronic health records or data repositories, for data analysis and to keep a history.

IoMT increases human-machine interaction which enhances the real-time health monitoring solutions and patient engagement in decision making. Table 1 lists the key benefits and drawbacks of IoT implementation in the healthcare domain. IoT enables the real- time health monitoring, data registration and health record maintenance to assist in the data driven decisions. These may provide a personalized health regime for the patient.

Table 1.

Advantages	Drawbacks
Patient Benefits • Real-time interventions in emergency situations • Cost reduction • Reduced morbidity and financial burden due to less follow up visits	Technical Challenges • Security of IoMT data - hacking and unauthorized use of IoMT • Lack of standards and communication protocols • Errors in patient data handling • Data integration • Need for medical expertise • Managing device diversity and interoperability • Scale, data volume and performance
Health and Care Providers • Optimal utilization of resources and infrastructure • Reduced response time in case of medical emergency	
Device Manufacturers • Standardization/compatibility and uniformity of data available • Capability to sense and communicate health related information to remote location	Market Challenges • Physician compliance • Data overload on healthcare facility • Reluctance of mobile health adoption • Security policy compliance

The key areas of technical impact for the use of IoMT are growing, but can be generally grouped their utility in these domains:

- Patient-specific care with context and enabled through past health records
- Real-time tracking and intervention
- Data driven health prediction
- Development of evidence-based guidelines which can helpful to incorporate the local intelligence in future machine
- Improved inter-device connection and synchronization

02 IoMT Applications that Provide Strategic Advantages in Health Care Delivery

2.1 Chronic Disease Management

IoMT-enabled devices offer promising alternatives to manage chronic morbid disease conditions such as hypertension, cardiac failure, and diabetes. Such devices are used to monitor parameters such as blood pressure, random blood sugar levels, and weight and electrolyte concentrations inside the body. The real-time vital data sourced by these devices is processed at a higher level and used for future treatment alterations and dose changes, and to predict the disease's progress. Furthermore, centralized data collection can be useful in studying the epidemiological trend in particular diseases in a specific population.

2.2. Remote Assisted Living (Telehealth)

Data from network devices is registered at a central location at the physician's office. Compiling and processing patient-specific data enables healthcare automation, which analyzes fresh data against past records and decides the future course to manage the patient. This machine-enabled intelligence helps service providers transfer the tasks of routing, monitoring, and field administration to IoMT machines, thus saving the cost incurred from implementing follow-up resources and infrastructure utilization. Additionally, remote monitoring has led to a decrease in member drop-out rates and increase in healthcare resource productivity. A number of service offerings of IoMT through commercialized systems have emerged for use in remote cardiac monitoring that separates the patient's identification information and observation data to ensure security. Furthermore, encryption protocols are used to transmit and store critical information, which ensures the reliability and security of the solution.

2.3. Wellness and Preventive Care (Lifestyle Assessment)

IoMT-enabled devices have facilitated health supervision with monitoring systems for diet, physical activity, and quality of life. Innovative devices, such as wearable devices, implantable chips, and embedded systems in biomedical devices track continuous data on patient activity and related vital changes. Advanced sensors, convertors, and firmware in smart devices allow users to analyze and correlate various vital events with health conditions at the local level. Additionally, the remote networking capacities of these devices provide expert assistance in emergency situations at any remote location. Existing medical devices can be modified into IoMT devices to sense real-time data for patient monitoring through enhancements such as sensors, signal convertors, and communication modems. IoMT devices have been conceptualized in various forms of smart wearable devices, home-use medical devices, point-of-care kits, and mobile healthcare applications, and are able to communicate with health care experts in remote locations. The convergence with other advanced communications, such as global positioning services, IoMT can overcome significant barriers to access and provide new access to integrated data streams with abundant opportunity to enhance quality and safety of care. Apart from their utility in managing regular health statuses, IoMT devices have also been used for disease prevention, fitness promotion, and remote intervention in emergency situations.

2.4. Remote Intervention

Real-time data obtained from sensors enables physicians to administer drugs and evaluate response in case of emergencies. Such timely interventions offer high-tech medical assistance particularly in highly specialized areas of acute care, such as neurology, surgery, and cardiac care. A similar demand feature that is luring of more IoMT is the likelihood of expanding access to care in outpatient settings and reducing the cost of hospitalization.

2.5. Improved Drug Management

IoMT-based RFID tags manage drug availability problems and supply cost. The FDA has suggested guidelines for RFID (Radio-frequency identification) and drug supply chain management. These include the addition of the tags on medication packaging, which enable manufacturers to ensure supply chain quality. Other solutions include adding this technology to medication; WuXi PharmaTech and TruTag Technologies have developed edible IoT “smart” pills, which help monitor drug doses and the patient’s pharmacodynamics and enhance pharmacovigilance. Such solutions may help drug companies mitigate risks and losses during supply chain and administration.

Other application areas of IoT with health care delivery implications include:

- Training courses and coaching representation to paramedical staff
- Assistance in rehabilitation and hospitalization
- Access to health information electronic health records (EHR) including personal health records (PHR) without loss of medical information
- Online protein analysis and accuracy of composition.

Considering the application areas above, the maximum potential to use IoT-based devices is in the field of chronic disease management. Table 2 illustrates end-application-wise projected savings due to the use of IoMT devices.

Table 2.

Application Domain	Health Conditions/Applications	Cost Saving Opportunities (USD) estimated
Chronic Disease Monitoring	Heart disease, asthma, diabetes, neurologic disorders	200 Billion
Telehealth	Remote care, dermatology, behavioral health, acute care consultations	100 Billion
Wellness and Preventive Care	Obesity, lifestyle change, sleep management, fitness, EKG (heart rhythm) tracking, smoking cessation, rehabilitation services, pain management, fall detection.	?

03 What Makes IoT Work

There are two basic options or forms of communication among devices that drive IoT. In both cases, they achieve data transfer by emitting a signal from a device and connecting it to other devices that are capable of receiving it and integrating the received signal into actionable outputs. The original form of this enabling internet connections is radiofrequency identification (RFID). More recently, the use of near field communications or Bluetooth technologies provide the same capability as RFID, however, they have the advantage of enabling devices to connect with each other without using the internet as a platform for communication.

3.1 Radio-frequency Identification Enabling Device Connectivity

Radio-frequency identification (RFID) refers to a technology whereby digital data encoded in RFID tags or smart labels are captured by a reader via radio waves. RFID is similar to barcoding in that data from a tag or label are captured by a device that stores the data in a database. RFID, however, has several advantages over systems that use barcode asset tracking software. The most notable is that RFID tag data can be read outside the line-of-sight, whereas barcodes must be aligned with an optical scanner. RFID belongs to a group of technologies referred to as Automatic Identification and Data Capture (AIDC). AIDC methods automatically identify objects, collect data about them, and enter those data directly into computer systems with little or no human intervention. RFID methods utilize radio waves to accomplish this. At a simple level, RFID systems consist of three components: an RFID tag or smart label, an RFID reader, and an antenna. RFID tags contain an integrated circuit and an antenna, which are used to transmit data to the RFID reader (also called an interrogator). The reader then converts the radio waves to a more usable form of data. Information collected from the tags is then transferred through a communications interface to a host computer system, where the data can be stored in a database and analyzed at a later time. In most devices, the RFID tag consists of an integrated circuit and an antenna. The tag is also composed of a protective material that holds the pieces together and shields them from various environmental conditions. The protective material depends on the application. For example, employee ID badges containing RFID tags are typically made from durable plastic, and the tag is embedded between the layers of plastic. RFID tags come in a variety of shapes and sizes and are either passive or active. Passive tags are the most widely used, as they are smaller and less expensive to implement. Passive tags must be “powered up” by the RFID reader before they can transmit data. Unlike passive tags, active RFID tags have an onboard power supply (e.g., a battery), thereby enabling them to transmit data at all times. These options bring flexibility to meet the demands of medical device needs.

3.2. Smart Tags

Smart labels differ from RFID tags in that they incorporate both RFID and barcode technologies. They are made of an adhesive label embedded with an RFID tag inlay, and they may also feature a barcode and/or other printed information. Smart labels can be encoded and printed on-demand using desktop label printers, whereas programming RFID tags are more time consuming and requires more advanced equipment.

3.3 Wireless Communications: Near-field Communications and Bluetooth

The advances in low energy emitting power supplies has brought new capabilities for medical devices. The implication of this means that devices in proximity can be connected without using the internet for the exchange of data. Generally, there are two approaches to signal emission and capture in IoT devices: Near-field communications (NFC) and Bluetooth technology. Bluetooth and NFC share the capability of excellent communication between devices over short distances. NFC is limited to a distance of approximately four centimeters while Bluetooth can reach over thirty meters. While it may seem that Bluetooth is superior in this regard, both Bluetooth and NFC technology have their advantages and disadvantages compared to one another and can work together to meet users’ needs.

NFC technology consumes little power when compared to standard Bluetooth technology. Only when NFC has to power a passive, unpowered source such as an NFC tag does it require more power than a Bluetooth transmission. The close proximity that devices connected using NFC must be to each other actually proves useful in crowded locations to prevent interference caused when other devices are present and trying to communicate. Bluetooth may have trouble dealing with interference when trying to send signals between two devices, especially when several other devices are in close proximity. Another benefit of NFC technology comes in its ease of use. Bluetooth requires users to manually set up connections between smartphones and takes several seconds. NFC connects automatically in a fraction of a second, so fast it seems instantaneous. Though the users must be close to one another to use NFC technology, it is faster and easier to set up than a Bluetooth connection. Bluetooth does still offer a longer signal range for connecting during data communication and transfers. NFC technology has taken advantage of this and can connect two devices quickly, then turn the signal over to Bluetooth so the owners can move further away without severing the connection. The latest development in Bluetooth technology, Bluetooth low energy (BLE), is targeted at low power consumption and uses even less power than NFC. BLE is one of the most important wireless technologies in application of IoMT. BLE systems have the advantage of power-efficiency, ease of application in embedded systems, and has widespread compatibility with smartphones. As the technology increases, Bluetooth and NFC technology may continue to work together, relying on each other to help users meet their data transmission needs.

3.4 Technology Supporting Design Needs in Health Care

The implications of the innovation in power supply and distance connections have importance in the manufacturing of medical devices when considering materials engineering characteristics and ultimate usability. Features for these devices include weight and mass, portability, compatibility with other materials, cost, and durability. Bluetooth and NFC advanced engineering are bringing flexible options to build medical devices that maximize impact in these performance areas, particularly for critical instrumentation that interacts directly with humans.

Traditional design principles have focused on uses in hospitals and clinics. However, the development of wearables or embedded devices for remote monitoring is now the major growth area in both consumer and medical device products. The convergence of wearable devices, smartphone enabled applications, expansion of broadband and wireless connectivity, and growth of telemedicine has been expanding the range of possible medical management opportunities in diagnosis and monitoring.

3.5. Local Systems and Control Layer of Data Systems

Decentralized intelligence is among the key elements of IoT. In decentralized intelligence, the prime objective is to build a medical device with intelligent control capabilities. This helps in processing operational data at the local level, in addition to the central server. These devices are usually enabled with sensors to measure operational parameters, converters to generate digital inputs, controllers to make real-time decisions based on inputs received from the converters, and network interfaces to share data with other machines or central servers. Examples of such devices are wearable monitors, implants, and physician handheld diagnostic devices. Compatibility and the integration of advanced electronics are additional factors driving the use of IoT solutions at the device level. Such devices are capable of acquiring qualitative, real-time biometric data from the patient’s body and transmitting it under a secured environment to a higher-level data architecture. Encoders, actuators, and encrypting devices perform data transformations and pass it on to the next layer of the ecosystem (i.e. communication protocols such as NFC and over-the-air programming) for analysis.

3.6. Device Connectivity and Data Layer of Data Systems

The layer primarily focuses on collecting data from the network device and storing it in predefined data stores. The technologies at this layer are not unique to any solution (such as patient monitoring). Secured medical data transfer technologies manage large data volumes and ensure quality during the process. Networking firms such as Cisco and Oracle are quite active in providing advanced technologies to user-end consumers and system integrators based on this requirement.

3.7. Analytic Solutions Layer of Data Systems

Irrespective of the types of healthcare solutions enabled, the central/remote server collects data from multiple devices over the network and their key components. The server with built-in algorithms analyzes real-time operational data to provide insights and conclusions. This data-driven diligence helps with diagnostic ability, disease prediction, and implementing preventive measures. The collective and comprehensive evaluation of data from different sources such as implants and smart devices enables healthcare solutions, such as remote patient monitoring, interventions, and chronic disease management.

Among the primary issues health care systems have to embrace when looking to the future is the convergences of a number of technologies. One of those aspects is the integration of information technology (IT) systems used for data-centric computing with operational technology (OT) systems used to monitor events, processes and devices and make adjustments in enterprise and industrial operations. The IT/OT convergence is at the heart of enabling edge computing. Edge computing is a way to streamline the flow of data traffic from IoT devices and provide real-time local data analysis instead of sending it across long routes to data centers or clouds. The advantage of doing this computing closer to the edge of the network lets organizations analyze important data in near real-time – a need of organizations across many industries, including manufacturing, health care, telecommunications and finance.

04 Market Landscape

4.1 Market Overview

The IoMT market is forecast to expand at a compounded annual growth rate of 37% and the technology adoption rate for IoMT will increase in coming years to grow the marketplace to reach USD 156 billion by 2020 and USB 2.4 to 6.2 trillion by 2025.[iii] Technologies used in IoMT can be divided into the three technical classes: local patient systems and controls include sensors, controllers, firmware, and end medical devices; device connectivity and data management comprise networking and database systems; and analytics solutions broadly consist of data analytics and cloud-enabled solutions and services. The major technology contributors in the IoMT ecosystem layers are firms that provide semiconductors and embedded systems; application developers; firmware companies; wireless network operators; data management companies; sensor, tele-presence, and location technology providers; internet security/privacy and machine-to-machine vendors; IoT service providers; and general telecommunication players. Currently, North America leads the market in the high penetration of medical technologies and coverage of IoMT services by government insurance policies. In future, analyst forecast growth of technology in Asia pacific and European market due to increasing awareness, changes in lifestyle, improved diagnostic facilities and disease burden.

Each layer comprises various sub-technologies that interact with each other for data flow between the patient and caregiver. Recent innovations in these sub-technologies are discussed in the following sections.

4.2 Local Patient Systems and Control Sensor and Smart Patient Devices

The conventional sensing device detects the various physiological parameters based on the potentiometric, accelerometric, and electrochemical principles. These sensors are incorporated within the medical devices and solutions. The recent shift in trend is toward the multi-sensing platform, which comprises a mix of two or more sensors in next-generation, personalized self-tracking devices. Multi-sensor-enabled products such as individual systems can be incorporated into existing devices such as smartphone applications and home automation sensors. Around 150 million wearable sensors and patches are estimated to be in use in the healthcare market by 2020 and smartwatches are likely to comprise about 50% of consumer wrist-worn devices.[iv]

Microcontrollers and gateways conventional controllers convert data from the analog to digital format. These devices include converters, which process and analyze the sensor data and convert it into biometric data, and then transmit this through a wireless network. The prime advantage of these devices is they reduce manual errors caused by human intervention. However, automating the data handling process may reduce accuracy, along with operational cost.

Recently, a longitudinal prospective study demonstrated the use of smart watches (Apple Watch Series) demonstrated the ability of an algorithm to detect atrial fibrillation thus demonstrating the medical utility of a consumer device to measure pulse rates using photoplethysmography.[v] In parallel, the U.S. Food and Drug Administration approved the use of the device as a Class 2 medical device.[vi]

Other peripheral technologies include graphic displays, controllers, gateways, and communication modems used for wireless data transmission from the patient's location to the physician's office. Some commercialized technologies include remote monitoring platforms (Freescale Home Health Hub); the Sonamba daily monitoring solution, which provides monitoring for the geriatric population (ZigBee®-based wireless connectivity for Sonamba); and the Numera Libris mobile personal health gateway. Future technological innovations are expected to focus on facilitating low power consumption and small device footprint, extending battery life, and furnishing bioenergy harvesting solutions.

4.3 Device Connectivity and Data Layer

Network technologies connect patient devices to remote locations and manage data transmission. These connectivity technologies are segmented into Wi-Fi, Bluetooth Low Energy (BLE), ZigBee, cellular, NFC, and satellite. Some implementations of wired and wireless technologies include Bluetooth® and Bluetooth Low Energy (BLE) (for personal area networks or PANs), used with personal devices, and Wi-Fi® and Bluetooth (for local area networks or LANs) in clinics or hospitals.

4.4 Analytic and Solutions Layer Continuous IOT Monitoring

Continuous patient monitoring provides the real-time tracking, feedback, and intervention of patient parameters based on real-time data obtained from connected devices. The market analyst estimates market growth for this sub-segment to be around USD 21 billion in 2016. Among the various commercialized platforms is the Masimo Radical-7®, a patient monitor for physicians' offices, which collects patient data and wirelessly transmits for ongoing display or notification purposes. The prime hurdles in enabling these solutions are related to the security and standardization of sensitive medical data across networked devices. Other data-driven solutions enabled in IoMT are medication management, chronic disease management, inpatient monitoring, and surgical intervention, which stem from remote monitoring.

05. Regulatory, Legal, and Social Aspects of IoMT

5.1 Cybersecurity

IoT technology introduces many new exciting opportunities and new applications. While IoT will make many novel applications possible, on the other side IoT increases the risk of cyber security attacks.[vii] Because of its fine-grained, continuous and pervasive data acquisition and control/actuation capabilities, IoT raises concerns about privacy and safety. Recent studies on some of the most popular devices in some of the most common IoT applications revealed an alarmingly high average number of vulnerabilities per device.[viii] On average, 25 vulnerabilities were found per device. This ranged from the devices lack of requiring passwords of sufficient complexity and length, to lack of encryption of local and remote traffic communications, and designs that included vulnerable user interfaces and vulnerable firmware. Multiple attacks have already been reported in the past against different embedded devices and we can expect many more in the IoT domain.

For medical applications, it is critical that solutions be adopted to ensure security, privacy, and safety of IoT systems with minimal impact on performance, scalability, and usability. Even though the computer and network security area has offered over the years many important techniques and methods, revisiting and extending these techniques and methods in order to address the specificities of IoT systems entails many scientific and engineering challenges.

Regulatory agencies in countries with abundant applications of IoMT are taking steps to address emerging cybersecurity and privacy concerns of medical devices. In 2017, the US FDA published a guidance on Postmarket Management of Cybersecurity in Medical Devices. This guidance is aimed at managing postmarket cybersecurity vulnerabilities for marketed and distributed medical devices. In addition to the specific recommendations in the guidance, encourages manufacturers to address cybersecurity throughout the product lifecycle, including during the design, development, production, distribution, deployment and maintenance of the device. Further, in 2018, FDA began a series of procedures to conduct pre-submission engagements for device manufacturers with regulators.

Further, a new set of critical infrastructure security recommendations from European regulators targets the IoMT manufacturer space. These recommendations have significant implications for medical device manufacturers and health technology developers' cybersecurity risk mitigation efforts ahead of a major data protection compliance deadline in 2018. The recommendations issued by the European Union Agency for Network and Information Security (ENISA), cover a broad array of industries including healthcare and medical devices. The ENISA report stems from the rapid growth of the IoT paradigm, which has spurred new and rapidly changing security risks, across government sectors, industries and healthcare systems worldwide. The report may also help companies including interconnected medical device manufacturers comply with the

European Union and United Kingdom General Data Protection Regulation (GDPR), a new data privacy law that took effect on May 25, 2018. Regulators point to the rapid rate of change in IoT technology and that this has outpaced the ability of the associated policy, legal, and regulatory structures to adapt, leaving no clear security framework to follow. This has led most companies and manufacturers to take their own approach when designing IoT devices, causing interoperability issues between devices from different manufacturers, and between IoT devices and legacy systems. Recommendations by the ENISA to improve industry positions in cybersecurity protections include the following:

- promoting harmonized IoT security efforts and regulations for industry;
- boosting awareness of IoT security's importance among industry, consumers, regulators and academia;
- refining secure hardware and software development lifecycles in the context of IoT;
- reaching consensus on interoperability across the IoT ecosystem;
- identifying and providing incentives for stakeholders to prioritize IoT security;
- establishing secure IoT product and service lifecycle management, and,
- clarifying liability issues among IoT industry and regulatory stakeholders.

The US FDA and ENISA guidance and recommendations have similar thrusts of emphasis thereby demonstrating a harmonized regulatory approach to the complex and evolving challenge of consumer and patient safety.

5.2 Privacy

The introduction of IoT for personal health information transfer in the consumer marketplace domain has many policymakers and regulatory authorities concerned about how the uses of data might be a gateway for nefarious applications. Control of data can be lost if someone hacks into the smartphone or computer acting as a remote for the other devices. In the case of computers and smartphones, this hacking can be done remotely and often undetected. Smartphones, just like computers, carry an enormous amount of personal information about their owners. They often link to bank accounts, email accounts, and in some cases household appliances and access to health or medical information is often conducted to gain access to financial data. As is the case with autonomous vehicles and their vulnerability to IoT hacking and malware, the potential implications of targeted medical devices is of concern for ransom and other personal harms using identifiable information.

In another sense, control can be lost as more and more companies collect data about users. This data often paints a detailed picture of individual users through the collection of activities online. Everything that an individual's searches and, for that matter, all of one's activities online, are likely being tracked by companies that use that data. These companies often use the data to improve the user's experience, but they also use this data to sell users products or sell to other companies who sell users products. This has spurred widespread policy concerns about individual privacy and uses of data for purposes not authorized by the individuals of whom it is about.

06 DISCUSSION

While IoT-based medical technology applications are still in a nascent stage of development, the implementation of connected devices could significantly improve healthcare delivery. Perhaps the greatest advantage would be an enhanced operational efficiency through a growing use of networked devices.

Transparent data flow from lower-level physical devices to the cloud (and associated data analytics) could enable real-time response from remote locations, perhaps saving lives now more than ever before. Data-driven decision making is likely to empower caregivers to accurately monitor a patient's comprehensive health status, take pre-emptive preventive measures, as well as instantaneously respond to emergency situations. The interconnected systems are forecast to reduce the burden of cost on patients, increase patient compliance, and leverage the advantages of smart devices that can provide instantaneous responsive healthcare.

Although automation in healthcare monitoring would increase operational efficiency, it may pose serious risks during implementation, such as data theft, insecure data transfers, and irregular network connections. These challenges, combined with regulatory hurdles, are projected to drive growth in IoT-based networking and data solutions. There is much to be done to advance the integration of IoMT into health care practices, particularly for remote monitoring and indwelling devices. For example, there is still a need to improve device and international data standards across the industry, which would enable data handling in a consistent fashion. Considering the benefits and associated challenges, IoMT seems a promising solution to improve healthcare monitoring and treatment outcomes. By providing individual data-driven treatment regimens and optimized devices as per physiological requirements, this technology represents a new era of personalized healthcare and better living standards the world over. Recent research and developments in sensors, networks, cloud storage and computing, as well as mobility, and big data analytics have evolved enough to enable the creation of affordable smart medical devices and a connected healthcare ecosystem

The rapid growth of IoMT in health care is prompting government leaders to rethink the means by which data are collected, valued, and used. Among the questions that policymakers are likely contemplating are the following:

- Might it be feasible to compare and contrast the policies and technologies involved in IoMT and electronic health records, with a particular emphasis on barriers to exchanging data among vendors and institutions?

- What are the most effective security safeguards to put in place when applying IoMT in the patient care setting with life-sustaining medical devices?

- What can the government and industry do together to raise the level of awareness about privacy and security that patients and providers should use when using IoMT?

- Is it feasible to develop strategies that catalyze innovative IoMT solutions to address public health needs and to support access to affordable and high quality health care?

- How might industry, academia, and government work together to establish the evidence necessary to support regulatory needs for market entry of medical products?

# # #

REFERENCES

[i] Leading the IoT: Gartner Insights on How to Lead in a Connected World (2007). Gartner Research

[ii] "I could be wrong, but I'm fairly sure the phrase ‘Internet of Things’ started life as the title of a presentation I made at Procter & Gamble (P&G) in 1999", Kevin Ashton, RFID Journal, 22 June 2009.

[iii] Manyika J., et al. Disruptive technologies: Advances that will transform life, business, and the global economy. http://www.mckinsey.com/insights/business_tehnology/disruptive_technologies. May 2013.

[iv] Dimitrov DV. Medical Internet of Things and Big Data in Healthcare. Healthc Inform Res. (2016) 22:156-163. DOI 10.4258/hir.2016.22.3.156

[v] Turakhia MP, et al., Rationale and design of a large-scale, app-based study to identify cardiac arrhythmias using a smartwatch: The Apple Heart Study. Am Heart J. (2019) 207:66-75. DOI 10.1016/j.ahj.2018.09.002.

[vi] https://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm620246.htm

[vii] Bertino E. Data security and privacy in the IoT. (2016) Open Proceedings. Proc. 19th International Conference on Extending Database Technology. https://openproceedings.org/2016/conf/edbt/paper-a.pdf

[viii] K. Rawlinson. Hp study reveals 70 percent of internet of things devices vulnerable to attack. http://www8.hp.com/us/en/hp-news.