IOT STANDARDS

IoT Standards Matters will look at different segments of the IoT market as it relates to implementation and use of standards. Each column will select a particular vertical, and lay out the relevant standards and technologies that affect the evolving IoT hyperspace. The pace of the columns will start broadly with the vision of narrowing the subject of subsequent articles toward more specific applications of standards, whether in the development, application, test, or commissioning of IoT technologies.

Introduction

It has been observed that the technologies developed by human beings in the past two to three centuries have had a major impact on earth's climate and nature's equilibrium. Some believe that we have reached a point of no return. This can have a huge impact on life on earth, especially on the human species. However, while technology has been responsible for most of it, technology also seems to have the solution to it. And IoMT (and ICT at large) has amply proved it in the last year when it helped mankind fight the Covid-19 pandemic in every aspect, be it business continuity, personal and social life continuity, tracing the spread of the virus, developing the vaccines at warp speed, or supporting hospitals and patient management. The lession: we need to change how we think about technology and innovation. Rather than allowing technological advancement to steer our narratives, innovation and technology should help us build bridges between the worlds we inhabit now and the ones we imagine for tomorrow.

Mentor's Musings on "Standardization Imperatives for Digital Transformation of Healthcare"

by N. Kishor Narang
Technology Philanthropist, Innovation & Standardization Evangelist

The current global challenge of the COVID-19 pandemic has surpassed the provincial, radical, conceptual, spiritual, social, and pedagogical boundaries. COVID-19 was announced as a Public Health Emergency of International Concern (PHEIC) in March 2020 and now it is recognized as a pandemic, and it continues to be a major public health threat worldwide. However, during the process of prevention and control work, it was recognized that digital technologies can play a critical role in combating COVID-19, and cover the entire life cycle of the health emergency, encompassing the following: prevention and preparedness, outbreak early detection, surveillance and response, recovery, rehabilitation, mitigation, etc.

The pandemic provided a veritable ground for field testing recently emerging technology concepts and practices, in particular, the Internet of Medical Things (IoMT) and digital health. The pandemic also led to interest in IoMT and digital health from a diverse range of innovation actors such as the technology design and finance community, governments, and regulatory agencies internationally. In the course of these seismic changes brought about by the COVID-19 pandemic, several opportunities and challenges have emerged.

Under the larger paradigm of 'Digital Transformation of Healthcare', the IoMT and digital health presently hold enormous potential for applications in healthcare because of the pervasive nature of ICT and IoT paradigms brought into focus by social distancing required to slow the pandemic, not to mention governments and the public seeking real-time approaches to health care.

The question most people would ask is: What do **standards** have to do with all this? Although most people do not realize it, standards and the methods used to assess conformity to standards are absolutely critical. They are essential components of any nation's technology infrastructure — vital to industry and commerce, crucial to the health and safety of citizens, and basic to any nation's economic performance. About 80 percent of global merchandise trade is affected by standards and by regulations that embody standards.

Standards enable us to pre-solve complex problems. International standards enable and provide society with efficient ways to get work done while maintaining the safety of producers who create and provide goods and services, as well as the end-users receiving the benefits from these goods and services, fewer technical barriers to trade and improved supply chains. Standards provide people and organizations with a basis for mutual understanding, and are used as tools to facilitate communication, measurement, commerce and manufacturing. Standards are everywhere and play an important role in the economy by facilitating business interaction.

Standards–Details of "Mega" Importance: The topic of standards and the challenge of effective standards development can bewilder, immersing the uninitiated in a blizzard of details. To some degree, this is unavoidable. After all, standards are details. They specify characteristics or performance levels of products, processes, services, or systems.

Standards are becoming increasingly important due to several intensifying trends:

- The pace of technological innovation is quickening.
- Trade volumes are growing faster than national economies.
- Business operations are globally distributed.

However, before discussing the role of standards in successful proliferation of IoT and IoMT in comprehensive, scalable and mature digital transformation of the healthcare ubiquitously across the globe, let us understand the IoMT and digital health landscape including, but not limited to, the market and technology trends and challeges and opportunities in the domain.

IoT 2.0 and IoMT

Since its advent more than a decade and a half back, the IoT paradigm has evolved through different phases of the famous Gartner Hype Curve, and has truly come of age, and it would be apt to see what the IoT 2.0 is, or could be, all about today.

"IoT", a concept that originally sounded like something out of a sci-fi movie – the "Internet of Things" – is, in fact, a reality, and one that is bound to become even more widespread, from being considered as one of the most disruptive technologies since the World Wide Web, to being on the verge of becoming one of the most profound technologies by weaving itself into the fabric of everyday life, until it becomes indistinguishable from it[1].

The IoT value chain is perhaps the most diverse and complicated value chain of any industry or consortium that exists in the world. In fact, the gold rush to IoT is so pervasive that if you combine much of the value chain of most industry trade associations, standards bodies, the ecosystem partners of trade associations and standards bodies, and then add in the different

technology providers feeding those industries, you get close to understanding the scope of the task. In this absolutely heterogeneous scenario, coming up with common harmonized standards is a major hurdle.

New technologies and paradigms like Big Data, Artificial Intelligence, Virtualization, Cloud Computing, MEMS,Human Augmentation (including prosthetics and wearables) are promising to disrupt the way we design products, systems and solutions. Design engineers need to develop new strategies that can help them navigate seamlessly through a much wider and complex canvas of technologies, ecosystems and stakeholders. It is difficult for innovation to happen across disjointed platforms and technologies. Creating the opportunity for ecosystem partners to work across common open platforms facilitates faster innovation.

The COVID-19 pandemic has highly impacted communities globally by reprioritizing the means through which various societal sectors operate. Among these sectors, healthcare providers and medical workers have been impacted prominently due to the massive increase in demand for medical services under unprecedented circumstances. Hence, any tool that can help the compliance with social guidelines for COVID-19 spread prevention will have a positive impact on managing and controlling the virus outbreak and reducing the excessive burden on the healthcare system.

IoMT has exponentially become more popular during the past decade due to the benefits for creating smart environments that can autonomously function to provide various services. IoMT wearable devices have been increasingly used for medical purposes, such as monitoring the health of the elderly, physical activity monitoring, and orthopedic care. However, most of the pre-COVID-19 uses of IoMT devices were for small-scale applications, and in many cases when the cost and scalability were not an issue. Given the large-scale challenges caused by the COVID-19 pandemic, autonomous services, and remote conducting of services (telepresence), have become of higher importance, in particular in the context of telemedicine calling for large-scale use of affordable and accessible technology which can be used in remote areas and in regions with limited economic power.

Deploying more automation and technology in hospitals such as IoMT bedside devices means fewer interactions with infectious patients and more staff protection. Readily available patient data will reduce the need and duration of hospital visits. This goes hand in hand with evolving technologies of remote doctor visits, remote diagnosis and monitoring. Although it is important to note as IoMT and automation rise, with the exception of pandemics, the technology does not replace the human-to-human connection, which is a crucial part of patient care. If anything, IoMT provides doctors with more time to focus on the human aspect of their jobs, such as patient and family consultations.

IDC estimated that more than 70 percent of healthcare providers are already deploying IoMT, which is good news for future pandemic prevention. The fundamental genius of IoT is that it turns any object into a source of data. In the case of IoMT, the "object" is medical, be it a heart rate monitor, a wheelchair, or a wearable device. A continuous stream of patient-generated health data (PGHD) can be used to analyze the health status of the patient. On a greater scheme, the collection of data from patient populations can be used to accelerate medical studies and development.

IoMT also enhances remote care for the elderly or those with chronic conditions, which in a scenario like the current Covid-19 pandemic, could mean a dramatic reduction of exposure to the most vulnerable populations. During a pandemic, caring for the elderly with the least amount of interaction is vital to avoid risking their lives. With virtual assistants, medical sensors, and smart homes, we can keep our vulnerable populations physically safe and mentally well.

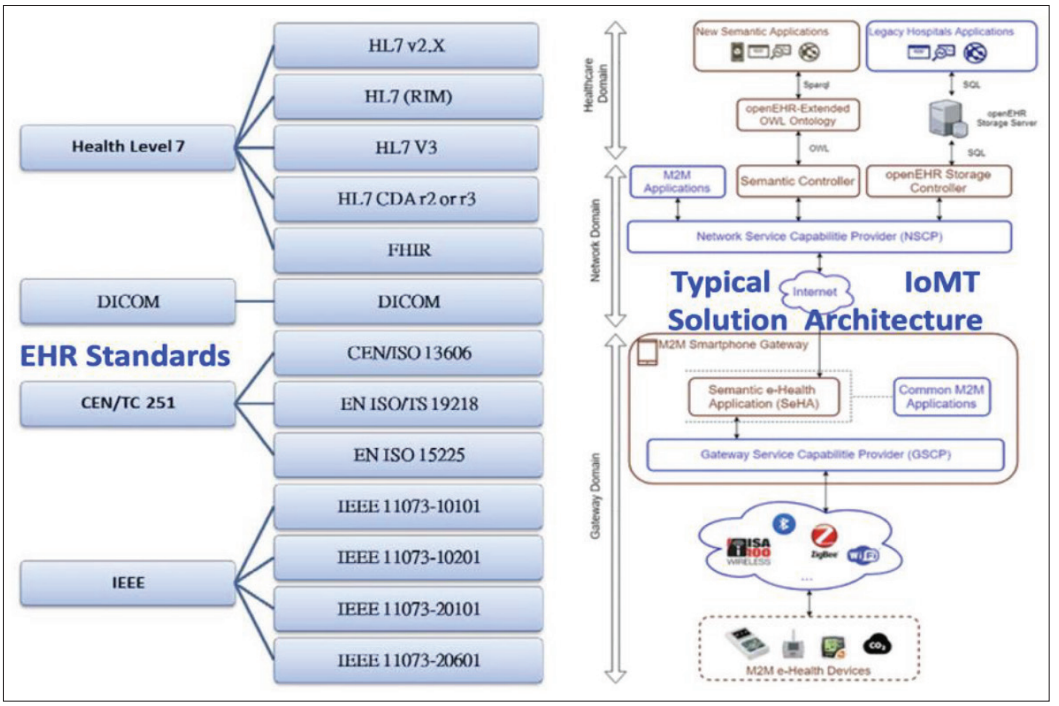
Cities, Infrastructure and Healthcare Management

During the COVID-19 pandemic, technological solutions have been critical in keeping our cities functional, and in fact the long lasting impacts of engaging technologies on urban areas may occur beyond COVID-19. Robots, drones, and contactless payments help with online shopping for food and pharmaceuticals, especially for the elderly and vulnerable communities. IoT-enabled control and automation systems help remote workers for manufacturers and businesses to deliver services. Online health consultations, online learning, and cultural services are possible due to high-speed affordable Internet that 5G cells offer for urban areas.

When a pandemic first breaks out in cities, early detection, isolating the infected person and tracing possible contacts are very critical. IoT protocols, particularly Bluetooth Low Energy (BLE) as well as NFC, RFID, GPS, and WiFi, are receiving much attention for providing solutions to these challenges. For example, these technologies have been used in wearables and disposable test cartridges for portable diagnosis. Here, we are still looking at the challenges with this digitization including computational time, data rate, coverage, energy consumption, cost and practicality.

Indeed, the closure of the hospitals to routine visits and fear of cross-contamination at the hospitals during the pandemic forced the public to seek other means of access to health care such as online consultations offered by smart phones and online medical staff. The new habits being formed during the pandemic thus call for further research, both conceptual and applied, to map the creative ways IoMT and digital health can be transitioned to practice, and how best to regulate digital health in times of both crisis and elective medical interventions. It is noteworthy that the prospects for real-time diagnosis, prevention, and intervention are challenged by the need to validate the digital health approaches in ways that are scientifically robust and socially just. At the same time, there is a need for research on digital health practices brought about by an unprecedented crisis with the COVID-19 pandemic on the planet. These include, for example, research on cost-effectiveness of digital health and the IoMT, and how best to balance local/planetary health priorities; social justice in the course of community implementation of digital health; applications of the IoMT in clinical trials and drug development for COVID-19, for example, to measure drug outcomes in real-time in real-life settings; and critically informed governance as required by all emerging technologies and applications for 21st century health care. The prospects for efficiency offered by the IoMT and digital health continue to be examined in the context of comprehensive trustworthy digital transformation of healthcare.

Even the Industry 4.0 ecosystem is preparing to confront the difficulties arising due to the COVID-19 pandemic. These advances can provide automated and computer-assisted services for our day-to-day lives during this emergency. Different advantages of Industry 4.0 that can be conceived for alleviating the impacts of the COVID-19 pandemic are: (i) manufacturing of prudent things identified with this infection; (ii) providing clinical assistance on time, utilizing the graceful chain; (iii) automating the clinical assistance and treatment to the infected patient to lessen the burden on specialists; (iv) learning from the experience and generate better machine learning models; (v)



EHR standards and a typical IoMT solution architecture.

providing a few developments with the assistance of advanced assembling and computerized innovations; and (vi) developing better hazard appraisal and worldwide general well-being crisis of this infection.

IoMT Landscape

A systematic use of smart wearable IoMT devices in various social sectors can intelligently help control the spread of COVID-19 in communities as they enter the reopening phase. The use of novel biosensors and intelligent algorithms embodied in wearable IoMT frameworks are now widely being leveraged for tackling this issue. With the use of smart IoMT wearables, certain biomarkers can be tracked for detection of COVID-19 in exposed individuals. Several machine learning algorithms which can be used to process a wide range of collected biomarkers for detecting (a) multiple symptoms of COVID-19 infection and (b) the dynamic likelihood of contracting the virus through interpersonal interaction.

Advances in artificial intelligence (AI) have accompanied the IoMT, for example, in a context of medical diagnoses using computed tomography scans for COVID-19 diagnosis. AI and big data had additional impacts on the course of the pandemic, for example, in logistics to locate and distribute much-needed medical supplies nationwide, not to mention the tracking of production and demand for medical supplies in the country.

The prospects and challenges already noted are also closely intertwined. A challenge can be transformed into a creative medical application that benefits public health, whereas the increases in efficiency of medical diagnosis and interventions call for critically informed technology governance and responsible innovation and in particular, to ensure individuals' and patients' rights and the collective action required to respond to the pandemic.

Such research ought to be accompanied by responsible innovation research on the governance of novel technologies and their reimbursement as well. The ongoing COVID-19 pandemic attests to the need for real-time data collection and big data sense making in a context of planetary health as well as innovation in technology governance that can collectively help cultivate responsible innovation in digital health and the IoMT. Digital health, the IoMT, critically informed technology governance, and responsible innovation should be considered as integral elements of the real-time pandemic response in the case of COVID-19 and other health threats that continue to impact society at large.

Several governmental funding agencies are now supporting research proposals across the world for designing low-cost scalable IoMT devices to enhance the health care system during the fight with COVID-19. The imperative is the need for having very low cost and effective IoMT devices for telemedicine which requires addressing a wide range of technical challenges including the accuracy, wearability, and ease-of-use (specially for the aged population) in unstructured dynamic environments and with minimum to no re-calibration needs.

For this there is a need for discussing the building blocks of an IoMT framework in the context of COVID-19. IoMT frameworks are composed of two cores, namely, hardware and middleware. The frameworks can benefit individuals and their medical correspondents by introducing Systems for Symptom Decoding (SSD), and the use of this technology can be generalized on a societal level for the control of spread by introducing Systems for Spread Tracing (SST). We can categorize IoMT technologies as (a) Systems for Symptom Decoding (SSD), and (b) Systems for Spread Tracing (SST).

IoMT-based SSD are those systems which assist with early diagnosis and tracing of the symptoms at the individual level while coupled with certain algorithms and additional hardware, SST technologies are technologies to model not only the individual symptoms but also the dynamics of symptom evolution in clusters of population based on interaction models and tracing of interpersonal interaction for better management of the spread in a cluster and on a larger scale in society. The challenges and potentials for the use of SSD technologies to continuously and autonomously monitor the vital signs of patients

can be to alert the individual and the care providers about any upcoming potentially major health anomalies so that proper medical care can be planned. The imperative role of machine intelligence, in particular health-related anomaly detection algorithms which can be used to not only detect but also predict flare-ups of symptoms, cannot be undermined.

Objective telemedicine sessions have been conducted with the use of SSD technologies, and this can be further promoted to enhance telemedicine quality and reduce the need for in-person visits, and to avoid interpersonal contacts. It should be noted that continual monitoring allows for detecting infrequent flare-ups of symptoms which may not be feasible based on infrequent discrete visits.

This is a major benefit of IoMT technologies which can significantly help with the fight against a pandemic, if low-cost, and highly accessible wearable IoMT can be made available. This will not only help with a faster and more efficient assessment of the symptoms, but it also will help to distribute healthcare resources optimally based on data collected from the affected patients. To further motivate more investment and investigation in this field, it should be noted that SSD systems can also significantly help to monitor individuals before the infection and promote early diagnosis, planning, and management under remote access. This will be possible due to the available infrastructures for a smart and connected healthcare model which should be further enhanced to prepare the system for future waves of the pandemic and future pandemics.

The use of IoMT devices can be extended to a higher level, for example, for clusters of patients in clinics or in small and then larger societies. This will be challenging but will allow monitoring not only the symptoms of individuals but also the spread of the symptoms. This concept has already been evaluated using smartphones in some countries (such as South Korea, India, and Iceland) and some states in the United States (such as Utah) using GPS data of smartphones to monitor COVID-19 spread. However, GPS is not precise enough to gauge short distances, especially for in-door interactions. Thus, other forms of technologies such as Bluetooth Low-Energy (BLE) have been suggested (for example, by Google and Apple) on smartphones.

However, despite the benefit of existing systems, such as BLE, the current technology has major limitations, among which we can highlight sensitivity to dynamic motions of the two carriers, sensitivity to a dynamic environment, the difficulty of calibration and need for re-calibration in a cluttered environment, and sensitivity to angle of arrival and location of the sender and receiver. This highlights a list of challenges that should be investigated for the higher performance of wearable IoMT on a large scale. Addressing these challenges, IoMT-based SST can implement preventive measures such as social distancing guidelines (SDG) based on the gathered multimodal information about (a) symptom evolution in a cluster of population and (b) interpersonal interaction in the clusters, especially in crowded indoor environments. Examples are medical facilities (such as dialysis clinics and neurorehabilitation clinics) and nonmedical facilities, such as nursing homes, senior homes, and drug rehabilitation facilities. On a larger scale, SST technology can enable medical providers to have broader symptom monitoring over the society (and clusters of the population) in terms of the pandemic spread, and thereby manage the distribution of hospitalizations and medical supplies. It can be mentioned that the extended surveillance that SST technology grants can help policymakers to detect and react to the main causes of the spread by enacting more accurate laws to fight against the spread. SST technologies also raise awareness among the people about the dangerous areas of the city in regard to COVID-19 spread.

Both SST and SSD technologies can be embodied as a personal smart wearable device to help process the related bio-signals for diagnosis, tracking, and prevention. However, this would require significant optimization of electronics and investigation of the means of reducing the cost to maximize accessibility and wide use of such technology among society regardless of the economic strength. This is a challenge to be addressed since most existing wearable systems either rely on connections with smartphones or have a very high cost, challenging the usability and feasibility of wide use in societies with a low economy. In addition, despite all the exciting benefits, data security and the reliability of data transmission can raise concerns and should be investigated thoroughly.

The Smart Watch: A Ubiquitous IoMT

While not originally designed as medical devices, smart watches are becoming increasingly powerful healthcare tools thanks to a range of applications and features that have been added to them by manufacturers such as Apple, Google and Samsung.

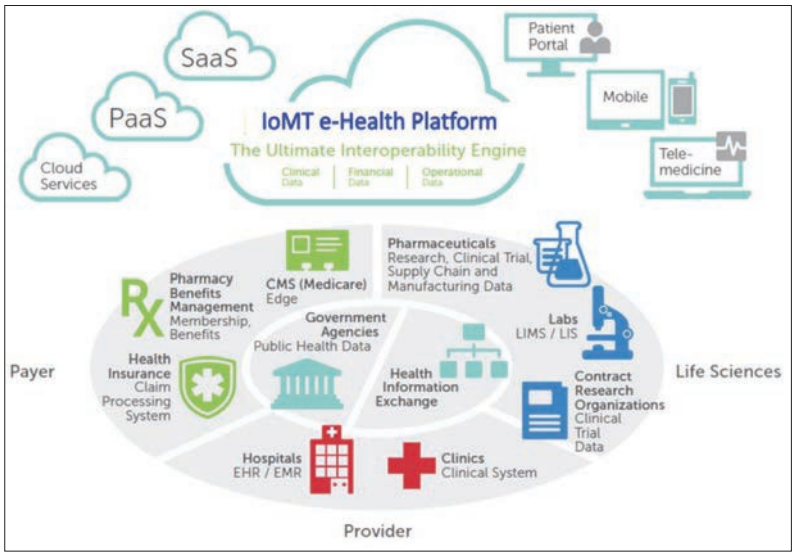
Apple in particular has consistently demonstrated a commitment to turning the Apple Watch into a device that can monitor and assist with health. In September 2020, the Apple Watch Series 6 launched with new blood oxygen measuring functionality, and Apple is reportedly embarking on a series of health studies with research institutes to learn more about how changes in blood oxygen levels can signal the presence of respiratory conditions such as asthma.

Since the launch of the Series 4, Apple Watches have also been able to take an echocardiogram (ECG) using an electrical heart sensor, and check for an irregular rhythm that could mean the wearer has atrial fibrillation (AFib), a heart condition that can lead to complications such as blood clots, stroke and other heart-related issues. An early 2020 clinical trial cast doubt on the Apple Watch's ability to detect AFib with much accuracy, and experts have also stated that widespread screening for conditions such as AFib, especially among the younger age groups who are likely to purchase a smartwatch, may not be necessary or particularly useful.

However, Apple has continued to improve the accuracy of its Apple Watch ECG, recently gaining FDA clearance for an updated version of the feature that can detect a category of the condition known as AFib with high heart rate. Samsung and Fitbit have also followed in Apple's footsteps in the years since the release of the Series 4 by releasing their own smartwatches with ECG applications, and the Samsung Galaxy Watch 3 also offers blood pressure monitoring, although it needs to be calibrated first with a dedicated blood pressure monitor, and every four weeks thereafter. The Galaxy Watch 3's ECG and blood pressure monitoring features were also initially only available to users in South Korea before being rolled out more widely.

Other simpler, yet still effective, health applications that have been integrated into smartwatches include sleep cycle monitoring and tracking, activity trackers and movement reminders, which can help combat excessive weight gain, and guided breathing and meditation exercises, which are beneficial to mental health. Apple, Google and Samsung have also all introduced handwashing apps and reminders since the onset of the Covid-19 pandemic that promote regular, thorough handwashing.

However, there are risks associated with integrating too many tools and features with a specific medical purpose into a gadget that is not specifically designed to be a medical device, as they can be less accurate, cause consumers to over-treat conditions that may not exist or be particularly serious, or prevent them from seeking true medical assessments with the proper equipment. On the other hand, it can be argued that making these tools more mainstream could prevent the onset of more serious conditions if symptoms are discovered early.



IoMT e-health platform.

There is also the question of data handling, and whether consumers should be putting so much of their health and biometric data in the hands of non-health specialists like Google (which also owns Fitbit), Apple and Samsung. Google for one has already been involved in multiple incidents involving the inappropriate or secretive transfer of medical data, such as Project Nightingale, and the DeepMind partnership with Royal Free Hospital. Companies have an obligation to be clear and transparent about the health limitations of their devices as well as how data will be used, while customers should make sure they read the fine print on their smart watches and go in with both eyes open.

IoMT Platforms for e-Health applications

The development of information and telecommunication technologies has given rise to new platforms for e-Health. However, some difficulties have been detected since each manufacturer implements its communication protocols and defines their data formats. A semantic incongruence is observed between platforms since no common healthcare domain vocabulary is shared between manufacturers and stakeholders. Despite the existence of standards for semantic and platform interoperability (e.g. openEHR for healthcare, Semantic Sensor Network for Internet of Medical Things platforms, and machine-to-machine standards), no approach has combined them for granting interoperability or considered the whole integration of legacy electronic health record systems currently used worldwide. Moreover, the heterogeneity in the large volume of health data generated by Internet of Medical Things platforms must be attenuated for the proper application of big data processing techniques.

The imperative is to develop standardized IoMT platforms that rely on semantic web concepts and M2M communications to simplify and standardize the development and integration of healthcare systems. It is crucial to consider data structures for the storage and transmission of data related to healthcare observations, which enables interoperability regarding data representation formats, IoMT platforms, and domain language (healthcare vocabularies).

The platforms need to leverage the openEHR-Extended ontology, which aligns the healthcare domain (openEHR) with the IoMT technical domain (SSN). It shall serve as a data storage model following a semantic WEB approach, but also identify sensors and automatically translates SenML sensed data to OWL individuals, thus granting semantic coherence between both domains.

The semantic extension of the openEHR model to the M2M Gateway domain, which enabled definitions of heterogeneous IoMT devices inside a unique data model through a relation between the openEHR Observation archetype ID observed by the device and the device definition inside SSN, is another critical imperative

Moreover, M2M capable IoMT devices can use their custom message format to forward sensed data over the M2M environment. Our platform addresses this problem and provides tools for the implementation of data converters in the SeHA deployed on the M2M Gateway, which converts heterogeneous data into a semantically coherent SenML format.

A comprehensive approach is also needed for performance tests and extensions to new scenarios, such as Smart Cities, where healthcare data plays a vital role in the creation of statistical indicators on the quality of life and the performance of cities. Moreover, for a Smart City implementation, the integration and interoperability among different verticals (transport, energy, environment, healthcare, and security, among others) represent an area that also needs to be addressed.

The Privacy and Security Conundrum

The discussion of IoMT and IoT in general is never complete without addressing security and privacy concerns. While IoT technology has evolved enough to carry data back and forth from objects to the cloud, device and data security remain an issue. This explains why healthcare providers have been deploying IoT in their back-end systems and are cautious with how much customer interfacing is mobilized by the new frontier of IoMT. Patients are rightfully nervous about a smart wearable medical sensor constantly broadcasting sensitive information about their health status. In addition, in the case of a pandemic and especially when it comes to contact tracing, data privacy becomes a sensitive issue. If we deploy Bluetooth tags in the population to enable contact tracing at the rise of a pandemic, who owns the collected data? And to what extent can this sensitive data be accessed and manipulated?

Privacy is a significant concern and must be addressed before any potential large-scale use of IoMT devices for contact tracing and symptom tracking. Without a systematic solution which provides a very high degree of protection of patients' data, IoMT devices can only be used up to a limited scale, such as for in-hospital uses or for clusters of high-risk population in a closed space (such as nursing homes to track symptom evolution in the population), or as part of telemedicine and individual uses. These are examples of limited scale uses for which the important matter of privacy and security can be addressed using existing infrastructures. For any large-scale use of the device, a serious concern that needs to be addressed is the matter of large scale security and privacy of the information. One additional issue related to this topic is the reliability of data storage and data transmission and accessibility of the medical sector to such data. Since Internet-based architectures that handle personal information can be a subject of different attacks, there is an imperative need for utilizing security algorithms. In addition to compromising information confidentiality, large-scale uses of IoMT architectures can increase the susceptibility to malicious cyber physical attacks that are aiming to hinder the processing of the data and causing failures, false-positive

alarms, and false negative reports. These attacks can range from low-level to intermediate-level and high-level. To address this issue, there is a need for implementing defense mechanisms.

While users of dedicated medical devices like wearable biosensors and hospital-issued pulse oximeters may feel comfortable sharing their health data with medical professionals, the issue of data privacy becomes murkier with devices manufactured by technology companies such as Kinsa, Apple or Google. Even if this data is being gathered for a beneficial purpose, can they be confident as to how it is being shared and used?

This is a trust hurdle that companies will have to continually battle and overcome as the use of the Internet of Things for healthcare purposes becomes more mainstream and accessible, and the number of available devices increases. Tech providers will need to demonstrate that they take privacy and anonymity seriously when they are handling and applying user data, and that they are only using it for strictly necessary purposes while taking the utmost precautions to maintain user privacy.

It is also incumbent on the consumer to make sure they are aware of the data they are sharing and how it might be used by the company in question. Health data is a particularly sensitive kind, and breaches of medical records can be serious. As we move increasingly into an age of technologically-enabled remote healthcare, it pays for consumers to be aware of where their data is going. While the benefits of improved health awareness, monitoring and care are immense, they should not come at the expense of privacy and data security.

Intrinsic Data Security Imperative in Healthcare to Earn Consumer Trust

The digital transformation of healthcare has been progressing at pace since the onset of the coronavirus pandemic; but in the midst of rapid innovation, earning the trust of consumers is still vital. After a year in which remote healthcare technology, or telemedicine, saw rapid and widespread uptake as a means of treating patients safely during a pandemic, the healthcare sector has made huge gains in terms of digital maturity. At the same time, there are still obstacles in the way of its transformation.

Healthcare professionals (HCPs) and patients alike have been willing to adopt health tech during the Covid-19 pandemic out of necessity; however, whether this pace of transformation will continue beyond the pandemic depends heavily on trust. Not just trust in the effectiveness of telemedicine, but trust that technology providers can be relied upon to safely and respectfully process health data, which is a uniquely sensitive category of data.

Healthcare is going to be a fascinating sector to watch in 2021 from a digital, data and technology perspective. We have seen lengthy healthcare digital transformation programs being cut in half during 2020. One crucial aspect of the Digital Transformation of Healthcare will be the role played by Data. In 2021 we will see healthcare organizations focus intensely on scaling, optimizing and measuring their services, but "trust remains the arbiter of data systems and is a precious commodity. The rush to solve the global pandemic using data and technology is placing great pressure on the foundation of trust as we move into 2021."

Since, telemedicine will have staying power even after the threat of Covid-19 has subsided, it will be important to understand how healthcare organizations should approach data in the midst of this "pivotal time", how they can demonstrate trustworthiness with consumers' most confidential information, and what other obstacles lie ahead when it comes to data and innovation.

What IoMT Cyber Security Learned from the First Wave

Healthcare organizations, such as hospitals and medical research institutions, have been hit hard by the COVID pandemic, and cyber criminals have, unfortunately, taken advantage of the situation. Attacks have risen by 300 percent since the pandemic started. If a lesson can be taken from the first wave of COVID, it is that the healthcare industry can take preventative measures to fortify clinical networks, preserve medical services, and ensure patient safety today and in the future.

In order to secure our hospitals, we have to look at why they are so targeted and difficult to secure in the first place:

- Personal health information (PHI) is extremely valuable on the black market, with a price tag in the thousands of dollars. By comparison, credit card and social security numbers can be worth as little as 10 cents.
- Connected medical devices, or Internet of Medical Things (IoMT) devices, are notoriously vulnerable to cyber threats. Many were not designed to connect to networks and do not have any built-in cybersecurity protocols. More than 70 percent of IoMT devices run unsupported Windows operating systems (e.g. Windows 7) that are no longer supported and cannot be patched.
- Standard security tools do not work for healthcare IoT. IoMT devices have unique communications patterns (think heart monitors communicating with nurse stations or MRI machines communicating with their vendor for routine maintenance). Without medical context, standard firewall and NAC policies could disrupt the normal function of critical devices and jeopardize patient safety.
- Clinical network topologies are in a constant state of flux. There are around 10 billion IoMT devices connected to the global clinical ecosystem today, with over 50 more connected each second, and 50 billion projected by 2028. The majority are connected without security checks, and thousands are moved between wards and off-campus sites completely unchecked. Keeping track of them all without an automated IoMT asset management solution is pretty much impossible.
- The variety of cyber attacks on healthcare has expanded. In the past, healthcare was typically targeted by sophisticated, state-sponsored attacks. Today, due to the vulnerability of the healthcare industry, amateur hackers carrying out simple, generic attacks on non-medical devices that happen to be connected to clinical networks (e.g., security cameras, PCs, game consoles) can cause serious harm. Hospitals need to be prepared for a variety of spontaneous attacks every single day.

COVID's Impact on IoMT Network Security

The pandemic has made the industry's cybersecurity challenges more complicated:

- Hospitals are understaffed, from medical staff to IT and cybersecurity professionals.
- Adoption of remote work and telehealth has spiked and is probably here to stay, expanding the attack surface of clinical networks and providing uncountable entry points for hackers.
- Equipment shortages alongside a surge of patients in crisis mean devices are hooked up to the network without any cybersecurity checks.
- Emergency quarantine units and field hospitals require cross-ward/cross-site equipment relocation, further expanding the attack surface and complicating complex clinical topologies.

Despite these hurdles, overcoming them is easier than it may seem. Healthcare organizations can solve the majority of their IoT cyber security challenges by taking preventative measures:

- Launch a cyber awareness campaign: For healthcare organizations, patients, and employees to stay safe, everyone from IT to medical professionals needs to be aware of cyber threats and cyber hygiene best practices.
- Adopt a zero trust security policy: By adopting a zero-trust policy, healthcare organizations can limit access to sensitive information such as ePHI (electronic personal health information) and reduce the attack surface. Zero-trust policies also help limit the reach of external attacks by stopping the propagation of the infection into sensitive devices on the network.
- Segment the network: Reduce the attack surface of the clinical network by limiting communications between devices to only those that are necessary to maintain medical services.
- Employ a Healthcare IoT security program: Automated security solutions can simplify and expedite healthcare IoT cyber security projects. They integrate easily with IT tools healthcare IT teams might already have in place and enrich them with the medical context hospitals need to avoid device downtime and ensure continuous clinical services.

The need for a Healthcare IoT security program is paramount in healthcare. Hospitals have a plethora of tools they can use right now to secure clinical environments exponentially faster than they would be able to manually. These tools simplify complex processes such as relocation, vulnerability management, and asset management with automated inventory and network segmentation capabilities.

Today's world may be plagued by things we cannot control, such as hackers stealing sensitive health information and a swelling wave of COVID infections. In spite of all that, we do have control over the steps we take to mitigate these threats. The tools and power to control healthcare's security posture and readiness for the second wave of COVID rests in hospitals' hands.

IoMT (IoT for Healthcare): Challenges and Opportunities

First, IoT deployment often comes with challenges around connectivity, power, spectrum and bandwidth requirements, as well as cost. However, the reduced cost of computing (including sensors) and increased mobile broadband penetration are expected to drive the use of IoT in healthcare. The cost effectiveness of standardized low-power wireless technologies will also help that trend.

Furthermore, large-scale deployment of the technology in healthcare relies on the transmission of health data and records, giving rise to privacy and security concerns. These concerns have propelled national IoT laws to be implemented in developed markets. However, there is still a need for effective regulations in developing countries to drive the adoption of IoT.

Finally, IoT-applied healthcare often comes with limitations. A large number of health issues require physical health examination to reach a diagnosis. Also, images and videos transmitted via IoT-powered telemedicine can be lacking high quality resolution, making physical healthcare necessary.

The pandemic has changed people and organizations in many ways and provided a new start for digital infrastructure development. New business models are being created to help organizations, health professionals and citizens understand the complexity of a disease and ensure preventive measures. The need for remote patient monitoring and the management of everything from medical supplies to industrial equipment has been proven, but IoMT is still facing many challenges:

- Health organizations and governments will need to use more sensors and networks to connect assets, processes and people on a larger scale.
- Enhanced connectivity will be essential to help improve performance and ensure the widespread development of IoMT technologies.
- Better data sharing will be necessary within public agencies, but also between public and private, such as public and private hospitals. Currently, we only have a fragmented view of the data.
- Changes to privacy regulations will need to be made in order to use people's data. We are going toward a medical revolution that will shake up individual freedoms and could lead to a huge ethical debate.
- The ability to process, integrate and streamline all that data at various stages of the public health response will be crucial to the success of the technology going forward. In that sense, AI will play an increasingly important role in IoMT as doctors will need to be kept informed, but not overwhelmed with data.

Standards for IoMT

The IoT/IoMT signal chain is comprised of sensors, signal conditioning Ckts, embedded controllers/processors, communication modules, gateways, data acqisition platforms in the cloud, data processing and analytics platforms and visualization, graphics and user interface applications (apps). And since IoT is considered "a global neural network of heterogeneous and aware devices interacting with each other to bring some insights to the users", standardization plays a vital role in making the IoMT solutions ubiquitous and interoperable. Interestingly, in the last five to six decades different ecosystems such as homes, smart buildings, smart grid/utilities, smart factories and smart healthcare, all evolved in siloes and developed their respective standards for communication protocols, data models and all other aspects. In fact, they form a very tightly interwoven and homogenous confluence of similar technologies being applied in different domains for a common cause of serving mankind and making planet earth "sustainable, resilient and secure".

As Andrew S. Tanenbaum said in 1990, "The beauty of standards is that there are so many to choose from!" In an ideal world, we would have exactly one standard for each task or interface. In reality, there are often overlapping or rivalling standards, driven by different vendor "camps", e.g., home automation: KNX/EIB, LON, BACnet, X10; wireless networks: Bluetooth, ZigBee, WLAN, EnOcean, Z-Wave; ECG file formats: DICOM, HL7 aECG, SCP-ECG. So what can a developer do? Support all standards? Too expensive. Wait for one standard to replace all others? May not happen. Implement a software abstraction layer that permits certain interfaces/standards to be replaced? Good if possible. Choose one standard and accept incompatibility with all others? Bad, but sometimes the only choice.

Standards and Interoperability

Interoperability is a key requirement for the success of any solutions on the market! Systems must be "future-proof", i.e., grow and adapt with the changing needs of the user over time. There is a very large variety of user needs, and no vendor can offer a "one size fits all" product. Technology must integrate with local infrastructure and service providers. Think of sensors, actors, and complete systems as "Lego building blocks": you want to combine them in different ways. This is only possible with stan-

dardized interfaces between systems and system components.

Interoperability must be addressed on multiple layers: ability to exchange bits and bytes (network); ability to exchange well-formed messages (syntax); ability to correctly understand the information (semantics); ability to correctly provide the desired services to the user (user perspective). This requires an agreement across vendors about interfaces between sensors, actors, and IT component interfaces between software components (services). This is what standardization is all about. Standards (both official and industry standards) are the most appropriate means for this purpose! Fortunately, we are not starting from scratch here. A multitude of standards already exists. However, standards and even SDOs are not at the forefront of industry, developers or users' minds. There are misconceptions on what standards are for, and the case for the use of standards has not been made. Liberalization and markets have a lot of great virtues, but they cannot create their own conditions of existence; they must be designed!

IoT/IoMT standards landscape.

Reasearchers and startups always offer an argument that "standards block innovation". Rather, the fact is that "standards help define the contours for structured innovation". However, if under the guise of innovation, you just want to define your own shade of greens, blues or yellows, then innovation itself shall need to be either understood by them or redefined.

The standards relevant to IoMT could be classified into semantic interoperability (data and information models); syntactic interoperability (data exchange, message formats and structures); interface standards to integrate seamlessly diverse sensors, sub-modules, products and systems into a ubiquitous solution for any healthcare use case or application. In fact, when designing or developing any IoMT solution, it it is unlikely to be any one standard, but rather a bouquet of standards since most architectures do not pick one standard but have a layered approach capable of using multiple standards in the portfolio.

The most challenging and crucial imperative for the global SDOs is harmonization of standards in diverse siloed ecosystems in light of the pervasiveness of convergence today and the need to share data frictionlessly among different stakeholders with common interests. Standardized protocols and regulatory controls will allow seamless sharing of information and data between various devices. This will help in managing security breaches and dealing quickly with them. Adoption of universal standards will result in faster and more efficient responses to any future disaster or pandemic.

Conclusion

Technology helps in the application of those preventive actions that will inevitably involve the control of people's movements, the detection of body parameters in public places, and the application of remote health. IoMT technology helps to prevent and limit the spread of the virus. Acting decisively and responsibly to implement the necessary preventive measures could be one of the great lessons learned.

IoT technology can lead the way in helping to prevent and manage current and future pandemics. The IoT, deployed at mass scale, offers humanity an unprecedented body of data and analytics in the face of pandemics. Controlling the spread of a disease becomes more efficient and can help us track, test, and treat entire populations with IoT technology.

IoT privacy and security vulnerabilities must be addressed before the technology reaches the hands of healthcare consumers. Addressing such concerns begs for the collective work of legislative, economic, medical, and technical players in the field. From a technical standpoint, a tremendous amount of innovation already exist to protect hardware and software devices against hacks. For example, Secure Vault technology generates a unique signature, like a birth certificate, for each wireless chip. This means the computations performed on the chip become only available to IoT service providers of the IoT service and not to nearby hackers. However, establishing consumer trust in how their personal data is handled by the providers remains an open issue.

The joint use of openEHR and Semantic Sensor Network semantics for the achievement of interoperability at the semantic level and use of a machine-to-machine architecture for the definition of an interoperable Internet of Medical Things platform is an overarching imperative to bring a comprehensive interoperability and seamless integration into diverse e-Health platforms and even with other platforms such as Smart Cities platforms, etc.

It is crucial to initiate an in-depth conversation between different sectors, including researchers, technology designers, providers, hospitals, and policymakers to not only examine approaches that can be implemented rapidly to adopt the existing technology and improve the health care system's diagnostic and preventative power using IoMTs, but also to examine the challenges and future directions of such technology in particular when the use is scaled-up to a societal level in order to fight possible future waves of COVID-19 pandemic and future pandemics.

Footnotes

[1] Mark Weiser, "The Computer for the 21st Century, Scientific American, Sept. 1991.