The Evolving Internet of Healthcare Things

By Jerry Power,
Executive Director, Institute for Communications Technology Management,
University of Southern California

Quote: "**Given the lack of an IOT VNA, todays practice often treats the IOT application and the associated IOT devices as a complete system overlooking the potential to create a web of networked intelligence**"

It appears that the healthcare industry is approaching another technology cross-road. As technology continues to get smaller, cheaper and faster, the standard practice has become to make devices, tools, and just about anything else "intelligent". At the same time, networking itself is becoming faster, more pervasive, and less expensive. Finally, software systems, which include databases, artificial intelligence, man-machine interface systems, and cloud services, are becoming increasingly more capable. Together, progress in each of these is having a compounding effect on healthcare delivery today and may ultimately change how healthcare providers interact with patients tomorrow.

Generally speaking, most technology driven advances tend to occur in compartmentalized and independent bubbles; progress achieved in one sector serves as an enabler for progress to be made in another. Properly implemented, technologies like the smartphones, EHR (Electronic Health Record), and even WiFi have allowed the healthcare industry to improve the level of care for patients, efficiencies for administrators, and returns for shareholders. However, in some cases, we limit the potential gains technology could offer by looking at these domains as compartmentalized disciplines.

For example, building an automated inpatient monitoring system for the hospital may improve operating efficiencies while improving patient care, but more could be accomplished if data from other administrative domains and consumer devices could be integrated to create a more holistic perspective. Capitalizing on this untapped data to bring incremental value to the healthcare industry is exceedingly difficult when these systems are run by different

administrations who have made independent solution purchasing decisions. Further, integration complexity problems can be expected to increase dramatically as the industry continues to shift to data-driven patient management paradigms. Consider a medical device developer who has created a next generation device that generates a plethora of patient monitoring data. Practically speaking, it is almost impossible for an IOT device developer to understand all the different ways the data can be used by a healthcare professional and limitations are imposed when the device is coupled to a specific application designed to support targeted functional need. If, instead, data collection devices were independent from applications, a single device could drive many different diagnostic applications and the issue becomes one of connecting data generators with data consumers. Concepts like VNA (Vendor Neutral Archives) have begun to move the industry in the right direction by allowing medical images to be filed with EMR systems for independent access by various applications, but this concept needs to be extended to include other IOT devices as well.

Given the lack of an IOT VNA, todays practice tends to consider an IOT application and the associated IOT devices as a complete system. This practice tends to couple IOT devices to specific applications. However, by linking devices to applications, the net effect is to create a series of IOT application silos that are individually managed. Operationally, this is a complex proposition because staff has to be dedicated to each silo or staff members need to become operational generalists that provide basic support to a larger number of applications. This same siloed architecture also tends to limit the healthcare professional's ability to leverage data across a broad infrastructure. If certain applications are only aware of a limited number of IOT devices, it may be necessary to duplicate IOT device deployments if a deployed device is incompatible with a new application.

Some IOT application providers have attempted to solve this dilemma by creating application layer APIs which allows their application to link with another, as long as the other application is willing to accept data from a third party. This creates a manageable hierarchy as long as the number of applications remains small. However, such an architecture begins to operationally suffer as the system scales to support a larger number of applications. In addition, because the connectivity is dependent on the behavior of the applications, each application can become a

reliability/performance choke points. Such stop-gap measures can be expected to proliferate until a VNA-type vision can be applied to healthcare IOT.

While VNA philosophies can be used to break the IOT application-device silos that are appearing, they will likely not be able to incorporate consumer-targeted medical data into their archives as native data. Consumer IOT devices do not generally live up to medical device quality standards. Comparing a medical holter monitor to data generated by a consumer device will likely lead to confusion unless the healthcare professional knows the source of the data and the validity/reliability of the data sourced from such a device. Further, the behavioral dynamics that govern consumer use of a monitor provided by the doctor for temporary use is far different from the behavioral dynamics at play when a consumer purchased IOT device is continually providing data to a third party. Consumers may expect incentives, direct control, and other benefits to accrue from these devices personally procured from outside the healthcare industry. As a further complication, these independent devices add another dimension to the security conversation given open nature of these markets.

The creation of an evolved architecture that allows vendor neutral data stores and integration of consumer and medical data into one repository may require additional extensions to current practices. VNA systems could be integrated into medical record management systems at different points in the information flow. However, inclusion of consumer data into medical data flows implies a need for a tool that can serve to route the IOT data into the medical data space AND also route it to one or more consumer-friendly applications. Given that the system needs to support data flows between a variety of end-points, the routing mechanism must be security aware so that misbehaving IOT devices (and applications) can be identified and isolated from the network. In addition, the system has to support the creation and management of trusted relationships between data end-points with an appreciation for the fact that trust is a dynamic and very personalized expression of acceptability.

The forces that will drive the shift from an application-centric IOT environment to an infrastructure-centric environment are the same as those that drove the evolution of the Internet, with the only real uncertainty being the velocity which drives such changes. It could be argued that the lack of an open IOT

infrastructure will confine the majority of health care IOT by the IT department's span of control. That is, if an IT department can enforce specific device and application deployment decisions, the need for an open IOT architecture can be reduced. However, such a dictated IOT support plan, limits ecosystem partnerships (linkages to independent clinics, surgery centers, ambulances, etc.), and impedes patient-centric participation (unless the hospital provides all needed IOT devices and support).

In an effort to expand our health care paradigm, it becomes important to look at healthcare in the context of the patient. Rather than diagnosing the patient based on information gathered at the doctor's office, the patient should be able to provide the doctor with information about the environment where they reside, work, and transit. Environmental data, including data from consumer quality IOT devices would allow the doctor to makes much more informed healthcare decisions. Further, as healthcare-focused artificial intelligence applications become common place, applying data analytics to the wealth of real-time data about individual patients will become common practice.

The reality of such a vision is technologically within our grasp, however, there are many non-technology driven issues that must be faced and conquered before it can be realized. First, everyone needs to become comfortable with the privacy and manageability of such a system – this is not to say that people have to change but instead means that systems have to evolve to accept and working within the individual's view of privacy. This is not an easy or straightforward task in that the people who generate this data (via their devices) need to be made comfortable with the fact that they have control over who can see their data and that they can easily extend or rescind data permissions based on their self-interest. In such a data centric word, patients have to be treated as health-care partners where they are providing data in exchange for services; this is a give and take relationship like any other partnership. And, like any such partnership, the amount of sharing that occurs is proportional to the level of trust that exists between the parties, and this trust must be developed and maintained over time for the partnership to be successful.

This paper has been submitted to CIOReview publication in a future issue of the magazine. An advance copy is being shared with the CTM community in an effort to stimulate increased dialog around issues of importance to the CTM members.

This issue of Perspectives on Business and Technology wishes to thank the following companies and organizations that have shared their views and made this paper possible

The views expressed in this paper are reflective of CTM's desire to increase the level of discourse related to technology's impact on business and businesses needs being addressed by technology. The views expressed in this paper may or may not reflect the views of the CTM members, the I3 members, or USC.