The "Internet of Things" and Healthcare

Steve Gravely, Esq., Troutman Sanders LLP[1]

I. Introduction.

The Internet has fundamentally transformed the manner in which people around the world communicate, interact and conduct business. The "Internet of Things" is transforming how people interact with devices in every aspect of their lives. In this article, we focus on how the "Internet of Things" is changing the healthcare landscape.

II. What is the "Internet of Things"?

A. Definition and Content.

First named in 1999, the "Internet of Things" (IoT) has been variously defined as the "interconnection of uniquely identifiable embedded computing devices [or smart objects] within the existing Internet infrastructure,"[2] "a scenario in which objects, animals or people are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction,"[3] and "everyday objects – such as household appliances, light bulbs, coffee machines, automobiles, personal devices and health devices – that have network connectivity and can send and receive data without human interaction."[4] The essence of this concept is that individual, connected, uniquely identifiable devices can interact over the Internet to monitor, record, and respond to changing conditions.

The first Internet appliance was a Coke machine at Carnegie Melon University in the early 1980s. Programmers could connect to the machine over the Internet and determine whether there would be a cold drink available should they decide to make the trip down the hall.[5] Since

---

[1] Mr. Gravely leads the healthcare practice at Troutman Sanders LLP, an international law firm with offices in the US and China. He specializes in health IT and other eHealth issues. He has led several national work groups on eHealth issues including the ONC workgroup that created the first multi-party data sharing agreement to support the Nationwide Health Information Network and is currently leading the effort to develop the legal framework to enable interoperability across different Health Information Exchange networks and vendor systems.

[2] Wikipedia, "Internet of Things," available at http://en.wikipedia.org/wiki/Internet_of_Things.

[3] Margaret Rouse, "Internet of Things," Techtarget.com, June 2014, available at http://whatis.techtarget.com/definition/Internet-of-Things.

[4] Erik Post, "Discovering the Internet of Things," Law Technology News January 1, 2015, available at http://www.lawtechnologynews.com/latest-news/id=1202678554856/Discovering-the-Internet-of-Things?slreturn=20150002142612.

[5] Rouse, *supra* note 2.

then, the devices have become smaller, more complex and capable of functioning without human intervention. Some examples of IoT technology are obvious and have become accepted parts of our daily lives, including:

- "smart" watches that track fitness and health;
- "smart" phones that can interact with home appliances, such as garage door openers or keypads, to open a door when the phone is within a certain range;
- heart monitor implants that monitor and record heart rhythms and transmit the data to remote monitoring centers; and
- cars with sensors that send alerts when tire or fluid pressure is low – or that drive themselves using sensor input from the environment and other smart vehicles.

New devices and new applications for existing devices are being created every day. The only limit appears to be the imagination of developers and entrepreneurs.

B. Scale.

The Internet has enabled growth of the IoT on an expansive scale. The growth consists of two components: usage and devices. Usage of the Internet is astounding. Qmee estimated that, during 2013, *in 60 seconds* on the Internet users upload 41 thousand posts every second on Facebook, upload 72 hours of video to YouTube, conduct 2 million Google searches, download 15 thousand tracks from iTunes, post 347 blog entries on Wordpress, create 571 websites, post 104 thousand photos on Snapchat, send 204 million emails, post 3,600 photos on Instagram and publish 278 thousand tweets.[6] Usage is growing exponentially. Qmee updated its infographic for 2014, and many of the numbers increased dramatically – to 2.66 million Google searches, 1,800 Wordpress blog posts, 277 thousand photos on Snapchat, 67 thousand photos on Instagram and 433 thousand tweets *every 60 seconds*.[7] One consequence of this astounding usage is that the volume of information flowing through the Internet, and being captured in databases, is multiplying rapidly and exponentially.

The IoT is also growing explosively. In 2012, Cisco estimated that almost 9 billion

[6] Online in 60 Seconds, Qmee, available at http://blog.qmee.com/qmee-online-in-60-seconds/.
[7] Online in 60 Seconds: A Year Later, Qmee, available at http://blog.qmee.com/online-in-60-seconds-infographic-a-year-later/.

devices were connected to the Internet, up from 200 million in 2000.[8] By 2020, between 50 billion (Cisco' estimate) and 75 billion (Morgan Stanley's estimate) devices will exist in the IoT.[9] These numbers equate to over six connected devices for every single person on the planet. Driven in part by cloud storage and application technology (and soon to be enabled by IPv6, which will provide vastly more IP addresses than the current protocol, IPv4), the IoT stands to become a global nervous system that envelops users in accessible and often invisible technology.[10]

III. How does the "Internet of Things" apply to healthcare?

The healthcare landscape is vast and includes several major components: the healthcare delivery system including hospitals, physicians, pharmacies, home health providers and long term care providers; medical device manufacturers; pharmaceutical companies; insurance companies; health and wellness products and services; and even national governments as both providers of services and payers. Each of these components is huge in its own right. The interaction of the IoT with healthcare is already the subject of countless articles and books and a comprehensive treatment of this complex topic is far beyond the scope of this article. However, one can argue that there are three fundamental ways that the IoT is affecting healthcare in 2015: patient treatment, disease management, and population health.

A. Patient Treatment.

1. Bringing technology to the bedside.

The acuity of hospital patients in the US has increased dramatically as more and more procedures and medical conditions are managed in non-hospital settings. This means that almost every hospital patient in the US will be connected to at least one medical device, normally an IV pump, and a patient will interact with many different devices, such as imaging and laboratory

[8] Rob Soderbery, "How Many things Are Currently Connected to the 'Internet of Things' (IoT)?" Forbes, January 7, 2013, available at http://www.forbes.com/sites/quora/2013/01/07/how-many-things-are-currently-connected-to-the-internet-of-things-iot/.
[9] Brian Proffitt, "How Big the Internet of Things Could Become," September 30, 2013, available at http://readwrite.com/#!/2013/09/30/how-big-the-internet-of-things-could-become#feed=%2Finfrastructure&awesm=~oj3jHsZI8rJE6c.
[10] For a visual depiction of the possibilities, *see* http://cloudtweaks.com/2014/09/cloud-infographic-internet-things/.

equipment, during their hospital stay. Medical devices and technology is a rapidly growing component of the IoT which means that bedside devices now have the capability to collect data real time and transmit that data to other devices, like electronic health records, using robust operating systems. For example, a hospital in France teamed with Microsoft and Capsule Technologie to create a system built on existing devices, such as blood pressure monitors, thermometers, blood glucose monitors and oxygen saturation monitors, to capture the disparate streams of data from these devices and populate the data into the hospital's electronic medical record in near real time. [11] The resulting system allows nurses to record monitor information from a single screen, streamlining workflow and reducing error. The hospital reported that nurses were able to record an average of 9 percent more data in the same amount of time, ultimately saving 27 minutes of time per day, 164 hours per year.

Another simple illustration of how technology can assist at the bedside is a mobile chemistry analyzer, which can be used by the patient at home for immediate, automated, cost effective analysis. The device is identified with that patient and can be programmed to automatically upload test results to a central remote monitoring location. Collection and aggregation of data in the cloud can simplify transmission of the critical information and create time efficiencies for physicians and patients.

2. Improvements in patient safety.

Smart devices have the ability to improve patient safety and quality. The above examples show how use of smart devices at the bedside can create efficiencies and improve speed of appropriate treatment. Other safety improvements include reduction of medical errors and elimination of duplicate tests, improvements that can be provided by devices when they are connected to one another, rather than operating independently. Today, a patient who is having surgery is surrounded by highly qualified physicians, nurses and technicians who are focused on

[11] Neil Jordan, "A healthy dose of data transforms hospital efficiency," available at http://blogs.microsoft.com/iot/2014/12/02/a-healthy-dose-of-data-transforms-hospital-efficiency/.

that patient alone. Once the surgery is completed, the patient is moved to a recovery room where other highly specialized personnel closely monitor the patient as he awakens from anesthesia. Shortly thereafter, the patient is moved to a surgical intensive care unit (SICU) where the patient is treated by yet another team of highly skilled personnel who are responsible for several critically ill patients. Each of these transitions of care creates the opportunity for errors in the transmission of patient data. [12] In the OR, multiple infusion pumps administer various medications to the patient, and various monitors, ventilators, and other devices are necessary to ensure the patient remains stable.[13] When transferring the patient, often the trigger to set up services for the incoming patient in the receiving area is as simple as a phone call, where the possibility of communication or transcription error is high.[14] These scenarios are ripe for error.

In addition to these dangerous errors, false alarms caused by non-integrated devices can cause inefficiencies and "false-alarm fatigue," which can lead to alarms being treated less seriously by staff.[15] The IoT provides the opportunity to use various standards (such as the Integrated Clinical Environment standard, or ICE) and protocols (such as the Data Distribution Service standard, or DDS) allowing for real-time data distribution from devices that can be integrated using a private network or a private cloud.[16] The SICU can be electronically informed of the medication that the patient requires and smart devices can be preconfigured with the correct settings. The risk of transcription errors or miscommunication is greatly reduced.

Another area in which the IoT promises to affect patient safety is in medical device performance category, as well as proactive replacement of units and fulfillment of supplies. For example, Aerocrine, a device used in hospitals and clinics to diagnose asthma and determine the likelihood of steroid responsiveness, is a very sensitive instrument that suffers performance issues if the temperature or humidity of its environment is not controlled leading to downtime

[12] Stan Schneider, "The Internet of Things Can Save 50,000 Lives Year," Electronic Design, January 21, 2014, available at http://electronicdesign.com/communications/internet-things-can-save-50000-lives-year.
[13] *Id.*
[14] *Id.*
[15] *Id.*
[16] *Id.*

and resulting in less precise treatment of patients.[17] By using cloud services to collect and process telemetry data, sensor data and environmental data, as well as serial numbers and number of airflow measurements remaining, the manufacturer can determine when devices are operating outside normal parameters and issue alerts.[18] The ultimate goal of the manufacturer's efforts will sound in the "bedside" category as well – Aerocrine hopes to ultimately be able to place a device in a patient's home to allow proactive monitoring of asthma, which could reduce visits to hospitals and clinics.[19]

3. Improvements in access for underserved areas.

The use of the IoT to provide healthcare services to remote or underserved populations has, to date, been more accepted outside the United States (in Africa, Haiti, and Indonesia, for example). Those efforts demonstrate that there is significant potential for usage of smart devices to treat patients and provide healthcare services in medically underserved areas. There are many models where devices in the IoT can improve access to medical services using technologies such as communications via telemedicine (text, Skype, local extenders); remote capturing of vitals, blood measurements, and other critical test data; provision of tools that can collect, store, organize, sort, and share personal health information; and tools that dispense generalized health and safety information, such as healthcare kiosks.[20] These tools do not require the physician and patient to share space, even for visual diagnosis or lab testing, and can provide vital information and feedback when a face-to-face visit with a physician is either not an option, or is only available at an ER. The ability to educate a population using interactive technologies such as kiosks located in key areas may be a means by which technology can reach underserved individuals even in the absence of reliable wireless or broadband capabilities.

---

[17] Thor Olavsrud, "Internet of Things Helps Asthma Patients Breathe Easily," CIO, November 25, 2014, available at http://www.cio.com/article/2852000/healthcare/internet-of-things-helps-asthma-patients-breathe-easily.html.
[18] *Id.*
[19] *Id.*
[20] NORC at Univ. of Chicago, "Understanding the Impact of Health IT in Underserved Communities and those with Health Disparities," available at http://www.healthit.gov/sites/default/files/pdf/hit-underserved-communities-health-disparities.pdf.

B. Disease Management.

The IoT has the potential to dramatically affect the treatment of those with one or more chronic conditions, such as hypertension, diabetes, COPD, and cardiac conditions – diseases that are both difficult to manage and expensive. Smart devices allow for remote monitoring of these conditions. For example, in 2014, the FDA approved the first permanently implantable wireless sensor enabling remote monitoring of pulmonary artery pressure, which is useful for patients with heart failure, in that it allows identification of problems and modification of treatment before a patient ends up in the ER.[21] The sensor records information, transmits it to an external unit, and forwards the data to the medical team.[22]

Similar monitoring technology is leveraged in a system containing an integrated insulin pump, glucose sensor, and glucose meter that can be used to ensure appropriate management of Type 1 diabetes.[23] Testing has begun on an artificial pancreas that incorporates data from a glucose sensor to release the appropriate amounts of insulin – using wireless connectivity among devices not only for monitoring, but for releasing medication in response to bodily conditions.[24]

Smart technology that is integrated in the IoT has the potential to deal with one of the most intractable issues in chronic care – the failure of patients to take medications as prescribed. One company has developed an ingestible sensor that will activate with chemicals in the stomach to transmit a signal to a patch worn on the patient's body. The patch detects the signal and transmits it to a mobile device, such as the patient's smart phone, where the information is stored and can be transmitted to a remote monitoring site for review by the patient's care team.[25] The sensor also documents various metrics to determine effectiveness of the medication regime.[26] Estimates are that technologies such as this may save the world's healthcare systems up to $36 billion by 2018.[27]

---

[21] Maria K. Regan, "Implantable Med Devices – 3 Smart Technologies to Watch," PTC, June 2, 2014, available at http://blogs.ptc.com/2014/06/02/implantable-med-devices-3-smart-technologies-to-watch/.
[22] *Id.*
[23] *Id.*
[24] *Id.*
[25] *Id.*
[26] *Id.*
[27] *Id.*

C. Population Health.

1. Disasters and public health emergencies.

Smart technology can be of great service in a disaster or other public health emergency because of its ability to enable interactions between agencies and the public at a critical time. Even more compelling is the potential ability of the IoT to collect and analyze population or environmental data to provide analysis of risk and disease spread in a time-sensitive manner. The CDC, for example, has solicited proposals to identify a single platform that can integrate, analyze, visualize and report on key surveillance, epidemiologic, laboratory, environmental, and other types and sources of data during emergency or routine investigations in an efficient and timely manner.[28] Such a platform would allow for consistent response, capturing of usable data, and near real-time access to event data for the CDC and its partners, which would improve both initial response and analysis of the event to improve future response.

2. Accountable care.

Another population level use of the IoT is monitoring of patients who are enrolled in an accountable care program to determine utilization of services, facilities, equipment, and more – essentially, tracking a population's use of medical resources. The data collected can be used to adjust usage schedules and streamline delivery of appropriate services, as well as to pinpoint other elements of the IoT that can be used in early diagnosis and treatment, or to improve quality and reduce costs.[29]

The potential uses of the IoT in healthcare are myriad, and stand to benefit all players in the healthcare landscape with greater capabilities, efficiencies, timeliness of information, and interconnectivity. However, as these powerful systems are deployed, it is important to be aware of their vulnerabilities.

---

[28] Jennifer Zaino, "Challenge Disease and Public Health Emergencies with Big Data Analytics," Big Data Forum, October 6, 2014, available at http://www.big-dataforum.com/928/challenge-disease-and-public-health-emergencies-big-data-analytics; *see also* CDC, Solicitation Number HHS-CDC-RFI-2015-DCIPHER (modified), October 24, 2014, available at https://www.fbo.gov/index?id=cad9ab7a72a05ed69d51af99c7604252.

[29] Charlie Isaacs, "3 Ways Hospitals Are Using the Internet of Things to Improve Patient Care," Salesforce Blog, May 13, 2014, available at http://blogs.salesforce.com/company/2014/05/hospitals-internet-of-things-patient-care.html.

IV. What vulnerabilities may affect healthcare's use of the "Internet of Things"?

A. The IoT Depends on the Internet and the Machines that Interact with It.

The Internet, wireless technology, and smart devices are all technologies that can fail, be disrupted, or break. Internet connections can go down, batteries can die, computers can be hacked, and information can be lost. If experts are able to disrupt the Internet capabilities across an entire country such as North Korea, it is clear that a key weakness of these technologies is their reliance upon a means of communication that cannot necessarily be assured. The more dependent that the healthcare system becomes on the Internet and the IoT to provide services, the more vulnerable it is to service disruptions. The energy sector has dealt with this key vulnerability for many years and has developed very sophisticated systems and processes to assure its cyber-security. The healthcare system has a lot of improvements to make in this area.

B. Targeted Attacks.

1. Organized crime.

Medical identity theft is a growing problem, with over 1.84 million victims in the U.S. as of 2013.[30] Indeed, health care data can be more valuable than credit card data to an identity thief, because it contains even more private personal information, such as social security numbers, dates of birth, full names, current and former addresses, insurance information, financial information, and other critical identification information of the patient.[31] With this information, an identity thief can create very credible false identities of both patients and healthcare providers which they can then use to submit fabricated healthcare claims or illegally obtain prescription drugs. On a less sophisticated level, the thief may simply use the financial and personal information from the medical record to access bank accounts or apply for loans in the victim's name. The FBI has advised healthcare providers that they are targets of organized crime and must take steps to harden their information systems. The vulnerabilities in the systems are not just about technology; people might be the greatest threat to a healthcare provider's data.

[30] Erin McCann, "Medical identity theft hits growth phase," Healthcare IT News, September 12, 2013, available at http://www.healthcareitnews.com/news/medical-identity-theft-numbers-grow.
[31] *Id.*

Not only can computerized systems be hacked, but employees with access to systems can be bribed or otherwise exploited – or they could even be the criminals. The healthcare sector must increase its vigilance over its ever growing amounts of information.

2. Terrorism.

The audience may remember an episode of "24" where a terrorist assassinated the Vice President by hacking his pacemaker. This scenario is actually plausible given the fast pace of implementation of new smart devices. Imagine a 20-bed ICU that uses wireless IV pumps, wireless vital monitoring, wireless aspirators, and more. If a terrorist organization were to disrupt the wireless signals for a significant amount of time, or to supply false signals, it would wreak havoc with the health of the ICU patients and there would likely be a lapse before staff discovered the issues. Patients would likely die. Given that the point of terrorism is to cause terror – fear and panic – in the general populace, such an event would have just that effect. It would cause panic among a population that trusts in the ability of its healthcare entities to take the best possible care of patients and do no harm. Is this farfetched? Perhaps, but it is certainly not inconceivable.

C. Immature Legal Framework.

There has been significant discussion about the extent to which the Food and Drug Administration (FDA) should be regulating any device that interacts with a person in some manner related to the person's health. In 2014, the FDA released the FDASIA Health IT Report, which suggested that no new or expanded regulations be imposed on health IT at the present time, noting that the Office of the National Coordinator for Health Information Technology and the private sector should play leading roles in creating the proposed framework for health information technology.[32] The MedTech Act introduced by Senators Orrin Hatch and Michael Bennet on December 4, 2014 provides that various IT and smart device items should not be deemed "devices" within the meaning of the Federal Food, Drug and Cosmetic Act. This

[32] FDA SIA Section 1125 IT Report to Congress, available at http://www.fda.gov/RegulatoryInformation/Legislation/FederalFoodDrugandCosmeticActFDCAct/SignificantAmendmentstotheFDCAct/FDASIA/ucm356316.htm.

would prohibit the FDA from regulating these IT systems and devices specifically including, clinical decision support systems, and low-risk EHR software.[33] Regardless of whether Congress passes this type of legislation, the FDA itself has backed away from extensive regulation of medical applications in the IoT. Since issuing guidance on mobile medical applications, the FDA has issued various clarifying statements that list various types of mobile apps that it does not intend to regulate, such as glucometers, blood pressure monitors, heart rate monitors, and weight monitors; immunization trackers; drug safety information apps; and mobile apps used by physicians to access EHRs.[34] Many applaud the FDA's restraint while others warn of dire consequences for patients. This debate is not likely to end soon. In the meantime, the IoT continues to grow exponentially. The possibility of adverse events involving patients and the IoT increases over time as does the likelihood of widespread data breaches involving health information that is regulated by HIPAA and state privacy laws. This immature legal framework poses substantial legal risk for those involved in the IoT and in healthcare. It is not clear that the magnitude of this risk is appreciated by those who are working in the rapidly developing landscape.

V. Where Do We Go From Here?

The IoT describes an incredibly compelling and dramatically different future for the healthcare industry with countless possibilities for changing the character of medical interaction and care. As persuasively argued by Dr. Eric Topol, author of "The Patient Will See You Now: The Future of Medicine is in Your Hands," a new model of democraticized medicine is taking hold, one in which the smart device is the corollary of the Gutenberg press, the tool by which a medium formerly controlled by an elite subset was disseminated to the masses.[35] The smart devices that make up the growing IoT – embedded in individual lives, connected through the

[33] HIMSS, "Senate Considers the MEDTECH Act, December 5, 2014, available at http://www.himss.org/News/NewsDetail.aspx?ItemNumber=35986.
[34] David Harlow, "FDA continues to detail types of mHealth apps it will not regulate," HealthBlawg, June 17, 2014, available at http://www.healthblawg.com/2014/06/fda-continues-to-detail-types-of-mhealth-apps-it-will-not-regulate.html.
[35] Eric Topol, M.D., The Patient Will See You Now: The Future of Medicine Is in Your Hands, Basic Books (New York, NY) 2015.

wireless Internet, able to access cloud storage and applications as well as robust individual and population EHRs – will undoubtedly be transformative, but we must at all times remain aware of the risks and costs inherent in this transformation. The pace at which the IoT is growing means that federal and state laws cannot keep up, which results in very challenging legal issues for the healthcare industry.

24343960v1