EDITOR: Irena Bojanova, US National Institute of Standards and Technology, irena.bojanova@computer.org

The Internet of Things in Healthcare

Potential Applications and Challenges

Phillip A. Laplante, *Pennsylvania State University*
Nancy Laplante, *Widener University*

The Internet of Things (IoT) is a collective term for any one of the many networks of sensors, actuators, processors, and computers connected to the Internet. Healthcare applications for the IoT can potentially deliver comprehensive patient care in various settings, including acute (in-hospital), long-term (nursing homes), and community-based (typically, in-home).[1]

An IoT has the potential to accurately track people, equipment, specimens, supplies, or even service animals and analyze the data captured. With patients attached to sensors to measure vital signs and other biometric information, problems could be more rapidly diagnosed, a better quality of care given, and resources used more efficiently.

Applications for Healthcare in the IoT

The following represent just a handful of IoT healthcare application systems.

For the bulimia (eating disorder) patient in a hospital or home care setting, sensors in the patient's room could detect increased body temperature or blood pressure, or even the odor of vomit. Sensors could be used to detect exercise abuse such as excessive cardio training or accelerated walking activity as compared to walking at a normal pace. This data could provide valuable information in the diagnosis and management of the illness.

Consider a patient with Alzheimer's disease. Here, an IoT could employ geolocation to prevent wandering or other unwanted mobility behaviors. Often, patients with Alzheimer's suffer from comorbidities with other diseases, such as hypertension (high blood pressure), macular degeneration, or diabetes. Therefore, appropriate interconnected devices could capture data for monitoring the unique signs and symptoms of these conditions.

Safety and violence are real issues in healthcare today. There are numerous accounts of horizontal violence—for example, nurse against nurse—but also of violence from visitors or family toward healthcare providers or patients. Although healthcare institutions are equipped with video surveillance systems, an IoT could be another layer implementing a zero-tolerance policy. For example, tracking the movement of staff, patients, and visitors could provide warnings of aberrant or threatening behavior. Biometric sensors could be used to detect signs of aggression or stress in people who are entering or reside in these settings.

Monitoring in hospitals can take many paths. Staff might try to keep certain equipment, such as an IV pump or oxygen tanks, in their unit for future use. In a hospital, scarce shared equipment such as EKG machines, IV pumps, and patient-controlled analgesia (PCA) medication pumps could be tracked via an IoT. In addition, the use of such equipment would be of interest to individual units and administration—as well as insurance companies, including Medicare—in documenting the need for additional equipment. An IoT could also be used

 Published by the IEEE Computer Society

to monitor equipment that needs to be refilled or calibrated, such as oxygen tanks, and to alert staff of such situations.

In an acute or long-term care setting, low-cost RFID or bar code tags allow many supplies to be tagged for scanning, making it easy to make charges to a patient's account. Such supplies can also be tracked using an IoT as they are either checked out from a repository or administered to a patient. In some cases, where an RFID tag is used, an item could be located more quickly, for example. Likely trackable items include one-time use supplies, such as dressings, catheters of different types, and personal care items. In a home setting, medical supplies could be marked with RFID tags to monitor use and alert the home care team when an item is being overused or supply is too low.

Researchers and practitioners envision many other IoT healthcare applications that could substantially improve patient care, optimize resource utilization, and save vast amounts of money—if only the systems could be built.

Challenges Ahead

The deployment of full-scale IoT systems for healthcare applications has not been reported in the literature. There are reports of experimental implementations—for instance, monitoring patients' biometric signs or identifying when a patient has fallen using accelerometer data.[2] To track workflow, Kyoto University Hospital implemented a real-time location system employing handheld barcode scanners, Bluetooth transmitters, a beacon relay system, and barcode tags on patients, nurses, and supplies.[3]

The absence of deployed systems in healthcare settings reflects both the novelty of the technology and the existence of significant problems. For example, there are technological problems, such as electromagnetic radiation effects and signal strength problems, inside hospitals. Changing the behavior of staff in acute and long-term care settings to cope with the new technology also presents some real challenges.

We stipulate that any healthcare system must be safe, and this quality must be incorporated into any system specifications in this domain. But one particular set of challenges to implementing real IoT healthcare systems must be addressed: security, privacy, and trust.

Security

IoT applications must be secure. Exposing any component of an IoT healthcare system to a hacker, whether a terrorist, disgruntled person, blackmailer, or any other malicious actor, can have deadly consequences. Many researchers are working on the problem of securing IoT systems completely, but because no system can be 100 percent secure, ethicists and medical, legal, security, and financial professionals must define and quantify acceptable risk.

Loss of Privacy

No class of exciting applications for the IoT epitomizes the tradeoffs between security and privacy and functionality and privacy more than those in healthcare. But privacy is of paramount importance because patients expect that certain private information will remain confidential. Therefore, IoT healthcare systems must allow for sharing information that is needed to provide high-quality care across the care continuum, while at the same time assuring privacy.

There are legal obligations to protect private information in a healthcare IoT. The US, for example, has the Health Insurance Portability and Accountability Act (HIPAA) of 1996, whereas systems in EU countries must comply with 1995's Data Protection Directive. There are other patient-specific privacy needs based on a wide range of factors, such as age, profession, religion, and personal preference. However, in today's high-tech healthcare environment, new concerns have been raised as to the relationship of HIPAA and the IoT that have yet to be resolved.

Trust

Information that is being delivered from sensors might appear to be correct, but could be corrupted somehow at the origin or during transmission, or deliberately altered by malware that can gain unwanted access to the IoT via the Internet. This corrupted information might then be used to make life and death decisions. How then, can we trust the information delivered to us in an IoT healthcare system? This problem has yet to be resolved.

Another form of trust relates to compassionate care. Caring is about a relationship, one that is forged between the patient, their family and community, and nurses and other healthcare professionals. Compassionate care for the sick is an expectation for all healthcare providers, but compassion is based on trust. For example, for the 14th straight year, nursing has been rated as the most honest, ethical profession.[4] This high rating has been built on a relationship that begins with trust and a personal connection with patients and the public. Nurses often struggle with balancing technology and patient contact, because technology can at times remove the nurse from the bedside. Conversely, technology has helped improve patient care by allowing for better assessment, surveillance,

and treatment. With the advent of the IoT in healthcare, nurses must incorporate technologies on many levels and determine the best use for their practice and how to use technology to achieve desired patient outcomes. Other healthcare professionals will have to do the same.

There are exciting applications of the IoT for healthcare that promise to enhance the patient experience, improve workflow, optimize the use of scarce resources, and provide substantial cost savings. But real, scalable systems have yet to be built, and significant obstacles must be overcome. These obstacles include technological issues, safety, and security, privacy, and trust.

The IoT is still a novel concept for most healthcare professionals, but its use in healthcare is inevitable. Although the IoT adds another layer to the debate of caring versus technology, we encourage deeper consideration of the benefits, and encourage nurses in particular to add their voices to the development and integration of technology. Nurses are at the patient's bedside and often are the ones who need to be most comfortable with these technologies. Patient tracking can occur through the IoT within hospitals and outside in our communities, where here again nurses will question whether technology is taking the "care" out of healthcare. Consider populations not easy to reach who are monitored via telehealth—although there can be less human interaction, nurses here are able to care for patients that otherwise would be forgotten. The IoT can allow for monitoring and communication that thus far has not been available.

In 2013, it was reported that there were two Internet-connected devices for each person, and predicted that by 2025, this number will exceed six.[5] As new IoT systems are developed and deployed, the challenge in healthcare is to improve patient care without a reduction in caring through reduced human contact with patients. IT

References

1. P.A. Laplante and N. Laplante, "A Structured Approach for Describing Healthcare Applications for The Internet of Things," *Proc. IEEE 2nd World Forum on Internet of Things*, to appear, 2016.
2. L. Catarinucci et al., "An IoT-Aware Architecture for Smart Healthcare Systems," *IEEE Internet of Things J.*, vol. 2, no. 6, 2015, pp. 515–526.
3. K. Sato et al., "Feasibility Assessment of Bluetooth-Based Location System for Workflow Analysis of Nursing Staff," *Trans. Japanese Society for Medical and Biological Eng.*, vol. 51, supplement, 2013, p. R-314.
4. "Nurses Rank as Most Honest, Ethical Profession for 14th Straight Year," press release, Am. Nurses Assoc. (ANA), 2015; www.prnewswire.com/news-releases/nurses-rank-as-most-honest-ethical-profession-for-14th-straight-year-300195781.html.
5. D. Skiba, "Emerging Technologies: The Internet of Things (IoT)," *Nursing Education Perspectives*, vol. 34, no. 1, 2013, pp. 63–64.

Phillip A. Laplante *is a professor of software engineering at the Pennsylvania State University. His research interests include the Internet of Things, software testing, requirements engineering, and software quality and management. Since 2010, Laplante has led the effort to develop a national licensing exam for software engineers. He received a PhD from Stevens Institute of Technology and an MBA from the University of Colorado, and is a Fellow of the IEEE and SPIE. Contact him at pal11@psu.edu.*

Nancy Laplante *is an associate professor of nursing at Widener University. Her research interests include healthcare applications for the Internet of Things, the image of nursing in media, and creating authentic presence in online nursing courses. Laplante received a PhD from Widener University. She is board certified in advanced holistic nursing. Contact her at nllaplante@mail.widener.edu.*