Building Caring Healthcare Systems in the Internet of Things

Phillip A. Laplante, *Fellow, IEEE*, Mohamad Kassab, *Member, IEEE*, Nancy L. Laplante, and Jeffrey M. Voas, *Fellow, IEEE*

Abstract—The nature of healthcare and the computational and physical technologies and constraints present a number of challenges to systems designers and implementers. In spite of the challenges, there is a significant market for systems and products to support caregivers in their tasks as the number of people needing assistance grows substantially. In this paper we present a structured approach for describing Internet of Things for healthcare systems. We illustrate the approach for three use cases and discuss relevant quality issues that arise, in particular, the need to consider caring as a requirement.

Index Terms— internet of things, healthcare, security, privacy, safety, caring

1 Introduction

A healthcare application involves delivering patient care across the healthcare continuum (i.e. hospital, homecare, long-term care facility). Healthcare applications that are connected to the Internet; also referred to as Internet of Things (IoT) applications in health care, have been widely forecast, investigated, and even deployed on a small scale. For example, some hospitals have begun implementing "smart beds" that can detect when they are occupied and when a patient is attempting to get up, sending this information over the network/internet to nurses [28]. The beds can also self-adjust to ensure that appropriate pressure and support is applied to the patient without having to be manually adjusted by the nurses. Another area where smart technology is being discussed as an asset is coupled with home medication dispensers to automatically upload data to the cloud when medication is not taken or any other indicators for which the care team should be alerted [1].

The IEEE IoT Community defines the IoT as: "… a self-configuring and adaptive system consisting of networks of sensors and smart objects whose purpose is to interconnect "all" things, including every day and industrial objects, in such a way as to make them intelligent, programmable and more capable of interacting with humans'' [2]. According to information technology researcher Gartner [27], there are more than 6.4 billion devices connected to the Internet excluding tablets, cellphones and computers. That number is projected to hit 20.8 billion devices by 2020, as everything from a coffee maker to a kid toy is hooked up.

Because it is constantly growing and changing, it is often more useful to discuss a purpose built system within the IoT, referred to as a Network of Things (NoT) [3]. A NoT can be described by five primitives proposed by Voas [3]:

1. Sensor -- an electronic utility that digitally measures physical properties such as temperature, acceleration, weight, sound (e.g. cameras and microphones),
2. Aggregator – a software implementation based on mathematical function(s) that transforms groups of raw data into *intermediate* data. Two actors in conjunction with Aggregator are:
   a. *Cluster* is an abstract grouping of sensors that can appear and disappear instantaneously.
   b. *Weight is* the degree to which a particular sensor's data will impact an aggregator's computation.
3. Communication channel – any medium by which data is transmitted (e.g. wireless or wired),
4. External utility (eUtility) – a software or hardware product or service which executes processes or feeds data into the overall dataflow of the Network of Things (NoT),
5. Decision trigger -- creates the final result or results from data concentrations and any other data needed to satisfy the purpose and requirements of a specific NoT [3].

The nature of healthcare and the computational and physical technologies and constraints present a number of challenges to systems designers and implementers. These challenges are complex and include the following concerns:

- political (e.g. funding, mandates),

- *P.A. Laplante is with Penn State University, Malvern, PA 19355. E-mail: plaplante@psu.edu*
- *.M. Kassab is with Penn State University, Malvern, PA 19355. E-mail: plaplante@psu.edu*
- *N. Laplante is with Widener University, Chester, PA 19013. E-mail: nllaplante@widener.edu.*
- *J. Voas is NIST, Gaithersburg MD, 20899, E-mail: jeff.voas@nist.gov*

- behavioral (i.e. desired functionality),
- physical (e.g. available technology),
- communications (e.g. available channels),
- logical (e.g. analytics, languages, tools),
- structural (e.g. patterns of architecture and design),
- ethical (e.g. governmental privacy protection standards).

For example, in 2013 the U.S. Food and Drug Administration (FDA) released its rule for unique device identification system for medical devices, which will help in organizing adverse event reporting by making recalls more straightforward in an effort to improve patient safety [4]. The rule centers around two core items, the first of which requires a unique number to be assigned to every model of a medical device. Secondly, the rule will create a public database of medical devices. The FDA hopes these steps will help to more quickly identify specific medical device malfunctions and assess whether a recall is needed [4].

In spite of the challenges, there is a significant market for systems and products to support caregivers in their tasks as the number of people needing assistance grows substantially. For example, it is projected that by 2020, the number of Americans who are expected to need assistance of some kind to be 117 million, yet the overall number of unpaid caregivers (e.g. family members) is only expected to reach 45 million. That makes one unpaid caregiver for every 2.6 persons needing assistance [5]. Therefore, a large market opportunity is presented by those people who are online and connected, and who would make use of technology that is intuitive and consumer-friendly to provide care. Yet, there is not enough technology that can meet caregiving needs. According to a recent study conducted by Project Catalyst and the Health Innovation Technology Laboratory (HITLAB) to better understand how caregivers are currently using technology [5], an average of 71.5% of caregivers reported that they are interested in using technology across 17 tested care-giving tasks if such technology exists.

In this paper we present a structured approach for describing NoTs for healthcare by defining general classes of system types, classifying the healthcare delivery settings, then using the structured approach to describing the elements for a particular use case. We illustrate the approach for three use cases and discuss certain issues that arise. We also discuss considerations for dominant quality requirements in IoTs for healthcare.

2 General Classification For Use Cases For IoT In Health Care

Healthcare can be delivered in three broad-based setting types: acute care, community-based care and long-term care. Acute care refers to a hospital setting where the caregivers are paid health care professionals. Community-based care is delivered in a home setting, where the patient is living in his or her own or another's home and where caregivers are either paid professionals or unpaid family members or friends. Long-term care refers to nursing homes, or other skilled nursing facilities where patients reside for weeks, months, years or for the remainder of their lives and where caregivers are paid professionals.

IoTs can be used to collect patient and other data in these settings, and aggregate the data using analytics and then reporting this information to caregivers and/or take some action (such as shutting down a faulty medical device). It would be futile to try to enumerate all conceivable IoT applications in healthcare since after completing any list new applications will be innovated. Instead we define three classes of use cases of healthcare IoTs: A) tracking humans (e.g. patients, caregivers, and family members), B) tracking things (e.g. medical devices, supplies, and specimens), C) tracking humans and things.

A. Tracking Humans

Class A systems involve tracking humans' data (e.g. patients, caregivers, family members) using IoT devices. Perhaps the most mature field for IoT in health care is patient data-gathering. Currently, telemetry monitors can automatically measure and send or upload EKG stats, core body temperature (CBT), blood pressure, urine output, etc. By monitoring these vital signs, healthcare professionals can detect and start care earlier for infectious disease, cancer, heart failure, etc.

Another example in this class involves tracking the physical location of patients in any setting (acute, long-term, home). From tracking wandering patients admitted to ER to tracking patients with dementia, the IoT could geo-locate patients with Alzheimer's disease, or self-destructive behaviors such as bulimia, cutting, or suicidal tendencies. Such tracking can already be accomplished with commercial GPS bracelets, but local proximity sensors connected through Internet or cloud based technologies could allow tracking inside of the facility or home, or outside these where GPS signals may not reach. Additionally health care providers working in high risk areas, such as mental health care, may benefit from

tracking for security reasons.

B. Tracking Things

The second class of systems involves tracking "things" in a healthcare setting in real-time. These could include medical devices, supplies, specimens and more. For example certain shared equipment found in hospitals is "scarce" (e.g. EKG machines, Intravenous pumps, intermittent pressure devices for prevention of thrombosis). Nurses and hospital staff may sometimes store the equipment so that they can access it when needed, however this can create a problem if another unit is in need of this equipment but cannot locate it. IoT could be used to track the location of such equipment. For example Airfinder [6] is a real-time location system for hospitals and other enterprises that uses Symphony Link technology to track supplies in an operating room or throughout an entire hospital or facility.

In acute settings; future IoT technology can also provide an analysis of the use patterns of hospital supplies or devices to assist particular units in documenting use and need for additional equipment and acuity of patients. In a community-based setting sensors could be placed to monitor usage patterns. For example, oxygen tanks or medication administration devices; IoT could assist in tracking the usage and need for replacement of supplies.

Most equipment has alarm features for various exceptions (e.g. readings exceed limits, refill, failure, time to calibrate, etc.). Frequent equipment alarms can cause nurses and staff to become desensitized to the alarms (so called "alarm fatigue") such that they do not react quickly enough to deal with the exception. A NoT could be used to help differentiate these alarms for more effective response scenarios and send the alarm to the appropriate health care providers who should respond.

C. Tracking Humans and Things

The applications in Class C involve a hybrid of Classes A and B. Taking the dimensions of care settings and IoT application classes yields 9 general use cases: acute (A, B, C), long-term (A, B, C), home (A, B, C).

3 Use-Cases Specifications For IoT In Health Care

To illustrate how the general framework helps describe these healthcare IoT applications, we consider three use cases involving:

- a patient with an alcoholic addiction,
- a patient with Alzheimer's disease, and
- staff or patient safety issue or concerns in a hospital setting

In each case we describe the situation from a healthcare provider's perspective then using the framework established, showing how a specialized IoT could assist in monitoring and patient care.

A. Alcoholism Use Case

Alcoholism is a long-term chronic disease in which a person has developed an unhealthy dependence on alcohol [30]. In the U.S., there are close to 14 million people who are either alcohol abusers or alcoholics [7]. Fortunately, no matter how severe the problem may seem, most people with an alcohol use disorder can benefit from some form of treatment. Research shows that about one-third of people who are treated for alcohol problems have no further symptoms 1 year later. Many others substantially reduce their drinking and report fewer alcohol-related problems [7].

In the early stages of the treatment phase, a patient may suffer from Alcohol Withdrawal Syndrome (AWS), which refers to the set of symptoms that occur when a heavy drinker suddenly stops or significantly reduces their alcohol intake. With AWS, a patient may experience a combination of physical and emotional symptoms which include one or more of the following [29]:

- Anxiety or jumpiness
- Depression
- Shakiness or trembling
- Irritability
- Sweating
- Fatigue
- Nausea and vomiting
- Loss of appetite
- Insomnia
- Headache [29]

Some symptoms of AWS can be as severe as hallucinations and seizures. At its most extreme, AWS can be life-threatening. Detecting the degree of severity of these symptoms is essential to adjust the treatment. Matching the right therapy to the individual is important to its success. No single treatment will benefit everyone in the Alcoholism case.

Many of the above AWS symptoms could potentially be monitored using a specialized NoT or non-Internet-enabled analytics. For example, a patient with AWS needs to be carefully monitored regarding trembling and irregular movement. Sensors can be strategically placed in the patient's home and used to pick up on accelerated and irregular walking or movement activity as compared to walking or moving at a normal pace.

In addition a patient can be monitored for episodes of vomiting by observing instances of bathroom use via an IoT. A sensor that can detect the odor of vomit could provide additional cues in the diagnosis and management of the AWS patient in home-care settings.

A NoT system can render a decision on the existence of AWS symptoms and the degree of such symptoms. If a patient has mild to moderate withdrawal symptoms, a healthcare provider may prefer to continue the treatment in an outpatient setting while prescribing some medications to reduce the severity of the symptoms, especially if a patient has supportive family and friends. If the symptoms are extremely severe, then the system may alert the case as a medical emergency that requires an acute setting. Table I depicts a simple construct for an AWS patient in a long-term or home care setting using an IoT.

TABLE I.
AWS USE CASE CONSTRUCT

	Model Element	Realization
1.	Sensor	Proximity sensor(s)
2.	Snapshot (time)	Once per minute
3.	Cluster	Set of (3) proximity sensors per room or hallway
4.	Aggregator	Determine severity of AWS symptom
5.	Weight	Room layout dependent
6.	Communication channel	ZigBee[1] compliant network of sensors or clusters or aggregator, wired (Internet) to eUtility.
7.	*e*Utility	Remote monitoring software (onsite – e.g. administration desk).
8.	Decision	Degree of existing AWS symptoms.

B. Alzheimer's Disease Use Case

Alzheimer's disease is the most common form of dementia, accounting for 60 to 80% of all cases [8]. Alzheimer's.org reports that 1 in 9 people age of 65 years and older has Alzheimer's disease. It is important to note too that 81% of people with Alzheimer's disease are age 75 or older. Safety is a key factor in the care of patients with dementia. Also, the average lifespan in general for all people continues to rise, with many surviving into their 80s and 90s. The costs associated with care of the patient with Alzheimer's disease are staggering. All of these statistics highlight the need for technologies to assist in monitoring and support of these patients, their families or caregivers, and health care providers.

There are a variety of symptoms that a patient with Alzheimer's disease can exhibit, some are more common in early stages while others appear later as the disease progresses. With the number of cases of the disease continually on the rise, the health care community has been seeking ways to assure safety and quality of life for the patient and caregivers. Caregiver burden is a real concern because of the stress and level of care often needed, with most of this responsibility falling to family or caregivers. As the disease progresses the patient can have difficulty walking and swallowing that will require additional monitoring and intervention to keep the patient safe.

The following are common symptoms of Alzheimer's disease:

- memory loss that disrupts daily life;
- challenges in planning or solving problems;
- difficulty completing familiar tasks at home, at work or at leisure;
- confusion with time or place;
- trouble understanding visual images and spatial relationships;
- new problems with words in speaking or writing;
- misplacing things and losing the ability to retrace steps;
- decreased or poor judgment,
- withdrawal from work or social activities;
- changes in mood and personality, including apathy and depression [8].

Any of these symptoms could potentially be monitored using a specialized IoT or other analytics, though some would be more difficult than others.

As the disease progresses, cognitive and functional abilities can decline. People may need help with basic activities such as bathing, dressing, eating and using the bathroom; lose their ability to communicate; fail to recognize loved ones; and become bed-bound and reliant on 24 hour care. When individuals have difficulty moving, they are more vulnerable to infections, including pneumonia which is often a contributing factor to the death of people with Alzheimer's disease [8]. Clearly this disease takes a toll on the patient and caregivers, and it is easy to see the need for technologies to assist caregivers at different stages of the disease.

Allowing the patient with Alzheimer's disease the best quality of life is a focus of care. Especially in early stages, patients need to maintain a level of independence therefore caregivers and health care providers must seek ways to keep the patient safe without taking away all independence. Additionally, it is important for the patient with Alzheimer's disease to remain socially engaged to stimulate brain health; the sensors again can be placed to avoid detection by visitors. Many patients with Alzheimer's disease also have co-morbidities (or disesases or conditions), therefore a sensor may also capture data for monitoring of other health conditions, such as hypertension (high blood pressure). Monitoring through sensors with IoT can be a means to do this. The sensors could be strategically placed to capture important data, but not be intrusive.

[1] www.zigbee.org

A study by Niemeijer et al. provided evidence to support the development of less intrusive forms of patient monitoring. GPS tracking devices and video surveillance were two technologies included in this study, as these have been touted to increase freedom for patients with Alzheimer's disease [9]. This ethnographic study interestingly resulted in two themes, with the second theme highlighting that patients felt stigmatized and felt they were being "watched." Sensors could be built into residential communities in order to be better accepted. For example, radio-frequency identification (RFID) chips could be inconspicuously embedded in the patient's clothing for the purposes of position tracking. Local proximity sensors could track the location and movement of patients. Health care providers could be notified of emergency situations, possibly even linking an alert to local first responders. Sensors could be placed in areas to detect movement and vital signs. If the patient is becoming more confused and is wandering, the sensor could detect a pattern of wandering. If the patient is becoming agitated, the sensor could be placed to detect increased heart rate or blood pressure; also assisting in detection of vital signs related to co-morbidities. By contrast, if there is a sudden drop in activity, this could signal apathy or depression of a patient who perhaps is becoming more sedentary and less social. A simple construct for an Alzheimer's patient in an acute or long-term or home care setting using an IoT in shown in Table II.

TABLE II
ALZHEIMER'S USE CASE CONSTRUCT

	Model Element	Realization
1.	Sensor	Proximity sensor(s)
2.	Snapshot (time)	Every 30 seconds
3.	Cluster	Set of (3) proximity sensors per room or hallway
4.	Aggregator	Determine location
5.	Weight	Room layout dependent
6.	Communication channel	WiFi network of sensors or clusters or aggregator, wired (Internet) to eUtility
7.	*e*Utility	Remote monitoring software (onsite or offsite – mental health nurse)
8.	Decision	Patient wandering or patient not wandering, dispatch assistance

Privacy becomes a real issue here, however as patient information is potentially being disclosed outside of the immediate care providers and across insecure technologies.

C. *Staff / Patient Safety Use Case*

Safety and violence are currently very important issues in health. There are numerous accounts of horizontal violence, for example nurse against nurse, but also of violence from visitors or family towards health care providers. The Bureau of Labor Statistics (BLS) reported that 2010 experienced a >13% increase in workplace violence over that for 2009 [10]. The violence ranged from verbal threats to homicide, and the BLS states that there are likely many more incidents that go unreported. The BLS stresses the need for a zero tolerance policy, with education of all staff and providers.

A NoT could be integral to a zero tolerance policy by providing another layer of protection. For example, proximity sensors with an appropriate aggregation algorithm could be used to detect signs of aggression or stress in individuals. A simple construct for a patient or caregiver safety use case using an IoT is shown in Table III.

TABLE III
SAFETY USE CASE CONSTRUCT

	Model Element	Realization
1.	Sensor	Proximity sensor(s)
2.	Snapshot (time)	Based on need (e.g. every minute for staff, more frequently for patients)
3.	Cluster	Set of (3) proximity sensors per room or hallway
4.	Aggregator	Determine aggressive behaviors
5.	Weight	Situation dependent
6.	Communication channel	Bluetooth network of sensors or clusters or aggregator, wired (Internet) to eUtility.
7.	*e*Utility	Remote monitoring software (onsite or offsite mental health nurse)
8.	Decision	Patient or staff in danger or patient or staff not in danger, dispatch assistance

RFID chips could be embedded in the lab coats of personnel and in the garments of patients in high risk areas, such as mental health facilities. While these implementations raise numerous collateral questions, such as the ethics of monitoring providers, the possibilities for implementation solutions seem to be within reach.

Health care institutions are equipped with video surveillance systems, however, the question arises as to whether other means, such as metal detectors, in conjunction with an appropriate IoT could provide additional protection against violence with a gun, knife or other weapons. Health care providers have debated this notion, with some believing metal detectors are against the culture of the acute care environment (because they are perceived as prison equipment) however others support their use.

4 CONSIDERATION FOR QUALITY REQUIREMENTS FOR IOT IN HEALTH CARE APPLICATIONS

When specifying the functionality for IoT healthcare applications, attention is naturally focused on concerns such as fitness of purpose, wireless interoperability, energy efficiency, and so on. Conventional requirements elicitations techniques such as domain analysis, Joint Application Development (JAD), and Quality Function Deployment (QFD) among others [11] are usually adequate for these kinds of requirements. But in healthcare IoT applications some quality requirements are probably of greater concern. Three particular quality requirements (namely security, safety and caring) are of special importance in

healthcare applications because of the sensitive, personal nature of the information. We explore these types of requirements further in this section.

A. Privacy Requirements

Privacy concerns have always been a crucial aspect of health care. Patients expect that their personally identifiable information will remain confidential and that health care providers will protect them. Similarly, IoT-based healthcare systems must assure privacy but allow for sharing of information that is needed to provide high quality care across the care continuum. Many of the devices used in a provisioned, specialized IoT will collect various data whether that surveillance is known or not [12]. If so, where does that data go? Who owns it? And why is it being collected in the first place? Sensors and surveillance will be huge concerns to overcome in order to argue convincingly for compliance when the economic benefits to healthcare providers are overwhelming for this technology.

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 addresses how a patient's personal health information can be used and shared to assure privacy but to allow for sharing of information that is needed to provide high quality care. HIPAA is an integral part of today's health care system, and no health care provider would argue its relevance. New concerns, however, have been raised as to the relationship of HIPAA and the IoT.

A Forbes magazine report calls for new federal baseline privacy legislation, built-in security for IoT devices, data minimization (storing less, not more data) and security breach notification [13].

In February 2016, the Office of the Privacy Commissioner of Canada released a 34-page report [14] outlining concerns for privacy and data as the IoTs continues to take shape: "The Internet of Things has been compared to electricity, or a nervous system for the planet, to illustrate phenomena that are at once pervasive, unseen and will become crucially integrated within the fabric of our society," states the report. "Several international experts, thinkers and technology builders are forecasting profound political, social and economic transformations; concerns about privacy and surveillance are chief among them."

There has also been a substantial amount of academic research considering IoT functionality versus privacy. For example, Winter conducted a survey of Hawaiin healthcare consumers in order to identify specific "practices that will be brought about by the IoTs that may be perceived as privacy violations"[15]. Essentially, Winter found that these consumers were willing to trade off some privacy for the perceived benefits of information sharing. Moreover, Thierer argues against rash, restrictive regulation in response to security and privacy concerns that could thwart innovation in applications (including healthcare) related to wearable IoT technologies [16]. And Walla discusses some of the issues of patient privacy in Internet hosted personal records that are not covered by HIPAA [17] and Mercuri considers regulations intended to improve health care data access have created new security and privacy risks along with regulatory complexity for patients and practitioners [18].

B. Safety Requirements

Safety concerns address questions such as: is the system operating as intended? Is the system providing needed levels of care? Is it providing unintended functionality? Can a malfunction of the system harm a patient?

Safety requirements for medical systems often derive from oversight agencies, for example, in the United States, the Food and Drug Administration (FDA).

Wallace and Kuhn studied 342 failures in medical devices based on data from the FDA. Their study helped identify approaches for using fault and failure information to improve device safety [26].

They also found that "known [best] practices may not be used at all or may be misused." Wallace and Kuhn also recommended that for requirements generation of safe medical devices that engineers should

- gather failure and fault data [from previous and related systems],
- understand the types of faults that are prevalent for a specific domain, and
- develop prevention and detection approaches specific to these issues [26].

The US Underwriters Laboratories proposed a fault-tree analysis approach for specifying hazards in wearable devices [19], and this approach would be appropriate for other medical and healthcare applications using IoT technology. Using traditional techniques for defining misuse and abuse cases would also be appropriate.

C. Caring Requirements

Caring can be described as an act, or a way to approach a patient. Caring can be a trait that one possesses, and often an adjective to describe what is perceived to be a "good" care-giver. Most nurses will be able to articulate their concept of caring if asked. Lachman highlights the pervasiveness of the link between nurses and caring by pointing out that "caring and nursing are so intertwined that nursing always appeared on the same page in a Google search for the definition of caring"[20]. For our purposes, we adopt caring as an adjective (functional quality) with the following definition: "displaying kindness and concern for others" [21].

Caring likely encompasses elements of the qualities of trust, reliability, privacy and more, but none of these, by themselves, capture the full essence of caring. Instead, caring is a super ility resulting as some composite of other ilities (and the system quality called empathy). One possible

hierarchical representation for caring in terms of these other ilities is given in Fig. 1.

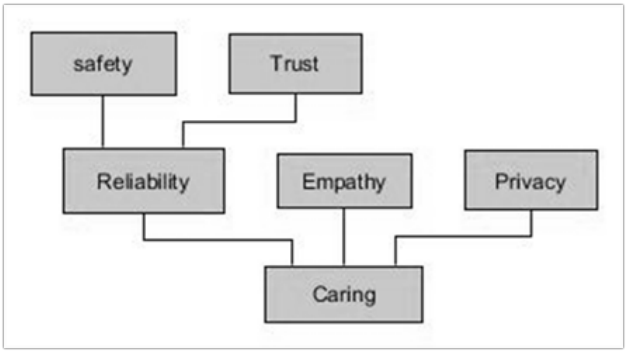

Fig. 1. A hierarchy of qualities related to caring.

Other types of systems may contain additional sub-qualities (e.g. usability, availability) forming a slightly different hierarchy than that in Figure 1. Since caring is comprised of some combination of other qualities that differ for each stakeholder and each system we find it convenient to express caring for a given system as a linear combination of these constituent qualities, which is: $\sum_{i=1}^{n} a_i q_i$, where the qi, are quantifiable values for the sub-qualities related to caring: such as safety, trust, reliability, and the a_i are weighting coefficients for these qualities. For each system C will be a "secret sauce" with the target goals for the q_i, related to system requirements to be specified.

"Caring" also means different things to different people and for different systems. Consider for example, a robotic surgery system. These systems are now used extensively for many types of procedures including heart, cancer and prostate surgery. While current systems are robotic in the sense that the machine mimics the movements of a human surgeon, fully autonomous robot surgical systems are envisioned in the near future, replacing surgeons and nurses in the operating room (OR) [31]. While we expect the human surgeon and nurses to care about the patient, as systems engineers, what should we require of a fully autonomous robot surgeon? Furthermore, what should the patient expect, in terms of a caring system, especially since the patient may be unconscious during the procedure? Their concerns are likely somewhat different.

Consider, for example, the constituent qualities of caring in the robotic surgery system. The surgeon wants the system to be safe and reliable, likely, as the primary concerns. Both the safe and trustworthy operation of the system contribute to a sense of reliability in the system and are of concern to the systems engineers. The patient shares these concerns but also wants the system to preserve his privacy (e.g. by not exposing medical records or embarrassing images). If the actors in the OR were humans, the patient would probably also expect a sense of empathy from the surgeons or nurses. Of course, robot surgeons look nothing like human surgeons, therefore there would need to be a means by which the robots could emote empathy via speech or facial expression generation on some display device. These diverse concerns, with respect to the qualities related to caring, will inform the specific system requirements discovery and representation process.

Very little work has been done to explore empathy in computing systems in comparison to other sub-qualities of caring. Brave et al showed that empathic emotion (via facial expression) in a computer agent interacting with a patient, has significant positive effects on users' opinions of that agent. They noted that "just as people respond to being cared about by other people, users respond positively to agents that care." Further they observed that the positive impression of caring was due to the "other oriented nature of empathic emotion; self-oriented emotion was found to have little or no effect on users' opinions of the agent" [22]. In another study Huang et al integrated Carper's nursing typology ("ways of knowing") and Locsin's nursing theory to define the "five senses of a caring robot." These five senses or qualities are: accurate recognition of nurse's instruction, confirmation of nurse's instruction, mid- to high-level "conversation competency", "motion competency", and the ability to demonstrate empathy, which they defined as a behavioral ability to convey empathy to a patient) [23]. Most other research that we found in affective computing investigated very specific examples implementations of technology and a situation (for example detecting a patient fall using wearable devices [24]).

Since many different definitions of caring exist, it is important to engage all stakeholders when trying to define a notion of caring for a new healthcare system and it is critically important to engage systems engineers, computer scientists, doctors, nurses and most importantly patients during requirements discovery. Many traditional requirements elicitation techniques could be used to uncover caring and related requirements depending on the size of the system. The most likely useful elicitation techniques for caring and related qualities, however, include surveys, interviews, prototyping (executable and non-executable), ethnographic observation, designer as apprentice [11]. Of course, different elicitation techniques may be used with different stakeholder groups, and multiple, complementary techniques should be used with each group.

For example, since empathy can be expressed via emoticons (e.g. Brave et al [22]) prototyping (of various facial feature displays, or voice outputs) could be used to generate empathy requirements. Interviews and surveys of patients could be used to capture desired caregiver behaviors (e.g. verbal cues, event triggered behaviors) that support patients in their belief that the healthcare system is trustworthy and safe. Ethnographic observation and designer as apprentice could also be used to elicit caring requirements by recording and analyzing the behaviors and movements of caregivers who are rated highly along the dimension of caring (there are instruments available from nursing theory such as the Caritas tool to do such measurement [25]).

Each quality requirement specification should be unambiguous and testable. In [32], the authors suggest to use a common form to specify quality attributes expressions. The form has six parts: Stimulus, Stimulus Source, Response, Response Measure, Environment and Artifact. In order to provide a guidance to requirements engineers when specifying Caring expressions, a set of possible values for each of the six parts is needed. This is a venue of research that we aim to pursue.

Of course, caring and related requirements that have been specified and delivered successfully in built systems could be re-used in related systems and in product lines. Other caring and related requirements may emerge from laws and regulations, for example in the robotic surgery system case, HIPAA. Finally, other requirements for caring and related qualities will eventually emerge as standards and reference architectures are developed for applicable systems (e.g. smart healthcare).

7 Conclusion

In this paper we introduced a structured framework for describing, and later help in specifying, designing and implementing healthcare IoTs. The approach involved defining general classes of system types, classifying the healthcare delivery settings, then using a structured approach to describing the elements for a particular use case. Using such an approach for describing (i.e. specifying) healthcare IoTs could lead to standardization, reuse, interoperability, best practices and so on. We also identified the need to consider "caring" as an important quality for IoT enabled healthcare systems.

Our work reinforced our belief that in planning IoT healthcare applications, there is strong need for domain expertise and deep inter-professional collaboration (in this case nurses and engineers). Engineers need nurses to assist with domain expertise, domain language understanding, patient advocacy, and point of care awareness. Nurses are involved in the day to day care of the patient in acute care and long term settings, and are the professional providers most often engaged in home care. Nurses need engineers to assist with technological insights, feasibility of use, and application and understanding of IoT for the benefit of patients, families, and providers. Clearly each professional brings expertise to the table but cannot create these applications in isolation.

Acknowledgments

This paper is a significantly extended version of Phillip A. Laplante and Nancy L. Laplante, "A Structured approach for describing healthcare applications for the Internet of Things," *2015 IEEE 2nd World Forum on Internet of Things (WF-IoT)*, Milan Italy, Dec. 14-16, 2015, pp.621-625. It received the best paper award at the conference.

The identification of any commercial product or trade name does not imply endorsement or recommendation by the National Institute of Standards and Technology, nor is it intended to imply that the materials or equipment identified are necessarily the best available for the purpose.

References

[1] R. Chouffani, "Can we expect the Internet of Things in healthcare?", available at http://internetofthingsagenda.techtarget.com/feature/Can-we-expect-the-Internet-of-Things-in-healthcare". last visited in November 2016.

[2] IEEE Internet of Things, available at http://iot.ieee.org/about.html , last visited in November 2016.

[3] J. M. Voas, NIST SP 800-183 Networks of 'Things': http://dx.doi.org/10.6028/NIST.SP.800-183 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-183.pdf, 2016.

[4] FDA News Release, available at: http://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm369276.htm?source=govdelivery&utm_medium=email&utm_source=govdelivery, 2013.

[5] "Caregivers & Technology: What They Want and Need", A report published by American Association of Retired Persons, avilable at: http://www.aarp.org/content/dam/aarp/home-and-family/personal-technology/2016/04/Caregivers-and-Technology-AARP.pdf, 2016.

[6] Airfinder, http://www.airfinder.com/, last visited in November 2016.

[7] National Institiute of Alcohol Abuse and Alcoholism, Treatment for Alcohol Problems: Finding and Getting Help, http://pubs.niaaa.nih.gov/publications/treatment/treatment.htm , last visited in November 2016.

[8] Alzheimer's Association (2015). 2015 Alzheimer's Disease Facts and Figures. http://www.alz.org/facts/overview.asp, last visited in November 2016.

[9] A. R. Niemeijer, B. J. Frederiks, I. I. Riphagen, J. Legemaate, J. A. Eefsting, and C.M. Hertogh, 2010. Ethical and practical concerns of surveillance technologies in residential care for people with dementia or intellectual disabilities: an overview of the literature. International Psychogeriatrics, 22(07), pp.1129-1142.

[10] United States Department of Labor, Occupational Safety and Health Administration, "Workplace Violence," https://www.osha.gov/SLTC/healthcarefacilities/violence.html, last visited 11/6/2016.

[11] P. Laplante, "Requirements Engineering for Software and Systems," Second Edition, Taylor & Francis, 2013.

[12] P. Laplante, N. Laplante, and J. Voas, "Considerations for Healthcare Applications in the Internet of Things," Reliability Digest, November/December 2015, http://rs.ieee.org/images/files/techact/Reliability/2015-11/2015-11-a03.pdf.

[13] T. J. McCue, "$117 Billion Market For Internet of Things In Healthcare By 2020," March 22, 2015, available at http://www.forbes.com/sites/tjmccue/2015/04/, last visited in November 2016.

[14] Privacy Commissioner of Canada report, https://www.priv.gc.ca/en/, last visited in November 2016.

[15] J. S. Winter, "Privacy and the Emerging Internet of Things: Using the Framework of Contextual Integrity to Inform Policy", Pacific Telecommunications Council Conference Proceedings, 2012.

[16] A. D. Thierer, "The Internet of Things & Wearable Technology: Addressing Privacy & Security Concerns Without Derailing Innovation", Available at SSRN 2494382, 2014.

[17] K. Walla, "Redefining "User-friendliness": Privacy Concerns Related to Non-HIPAA Covered Internet Personal Health Records", Unpublished, http://law.uh.edu/healthlaw/perspectives/2008/(KW)%20PHRs.pdf..

[18] R. T. Mercuri, "The HIPAA-potamus in health care data security."Communications of the ACM, vol. 47, no. 7, 2004, pp. 25-28.
[19] S. Kirk, "The Wearables Revolution: Is Standardization a Help or a Hindrance?: Mainstream technology or just a passing phase?", Consumer Electronics Magazine, IEEE 3.4 (2014): 45-50.
[20] V. D. Lachman, "Applying the ethics of care to your nursing practice," MEDSURG Nursing, vol. 21, no. 2, 2012, pp. 112-116.
[21] Oxford Dictionary, "caring," (n.d.) retrieved from: http://www.oxforddictionaries.com/us/definition/american_english/caring.
[22] S. Brave, C. Nass, and K. Hutchinson, "Computers that care: investigating the effects of orientation of emotion exhibited by an embodied computer agent", International journal of human-computer studies 62.2 (2005): 161-178.
[23] S. Huang, T. Tanioka, and R. Locsin, "Functions of a caring robot in nursing", 7th International Conference on Natural Language Processing and Knowledge Engineering 2011.
[24] Y. Cai, "Empathic computing," Ambient Intelligence in Everyday Life, Springer Berlin Heidelberg, 2006, pp. 67-85.
[25] J. Watson, "Core Concepts of Jean Watson's Theory of Human Caring/Caring Science," 2010, retrieved from http://watsoncaringscience.org/files/Cohort%206/watsons-theory-of-human-caring-core-concepts-and-evolution-to-caritas-processes-handout.pdf.
[26] D. Wallace., and D. R. Kuhn, "Failure modes in medical device software: an analysis of 15 years of recall data", International Journal of Reliability, Quality and Safety Engineering 8.04 (2001): 351-371.
[27] Garthner Technical Research, Internet of Things, Available at: http://www.gartner.com/technology/research/internet-of-things/, last visited in November 2016.
[28] R. Babu, and K. Jayashree. "A Survey on the Role of IoT and Cloud in Health Care." International Journal of Scientific Engineering and Technology Research 4, no. 12 (2015): 2217-2219.H
[29] Healthline, Alcohol Withdrawl Syndrome, available at: http://www.healthline.com/health/alcoholism/withdrawal#3, last visited in November 2016.
[30] Alcohol Rehab Guide, https://www.alcoholrehabguide.org/alcohol/, last visited in November 2016.
[31] C. Bergeles and G.-Z. Yang, "From passive tool holders to microsurgeons: safer, smaller, smarter surgical robots." IEEE Transactions on Biomedical Engineering, vol. 61, no. 5, 2014, pp. 1565-1576.
[32] L. Bass, P. Clements, and R. Kazman, "Software Architecture in Practice", 3rd ed, Addison-Wesley Professional, 2012.

Phillip A. Laplante is Professor of Software Engineering at The Pennsylvania State University. He received his B.S., M.Eng., and Ph.D. from Stevens Institute of Technology and an MBA from the University of Colorado. From 2010-2016 led the effort to develop a national licensing exam for software engineers. He has worked in avionics, CAD, and software testing systems and he has published 33 books and more than 200 scholarly papers. He is a licensed professional engineer in the Commonwealth of Pennsylvania and a Certified Software Development Professional. His research interests include software testing, requirements engineering and software quality and management. He is an IEEE Fellow.

Mohamad Kassab is an assistant professor in Software Engineering at Penn State Great Valley. He received his Ph.D. degree in computer science from Concordia University in Montreal, Canada. With more than 17 years of industrial experiences, he worked in different roles before establishing his career in academia, among which: senior quality engineer at SAP, senior associate at Morgan Stanley, senior quality assurance specialist at NOKIA, senior software developer at Positron Safety Systems. Dr. Kassab's research interests include developing a formal, integrated and quantitative approaches, architectural frameworks and tools to modeling and assessing software quality requirements.He is a member of the IEEE.

Nancy A. Laplante is Associate Professor of Nursing at Widener University teaching in the undergraduate and graduate nursing programs. She earned her BSN from William Paterson University, her MSN from West Chester University, and a PhD from Widener University. Dr. Laplante is board certified in advanced holistic nursing. Her research interests include health care applications for the Internet of Things (IoT), the image of nursing in media, and creating authentic presence in online nursing courses.

Jeffrey M. Voas is a computer scientist at the US National Institute of Standards and Technology (NIST) in Gaithersburg, MD. Voas co-authored two John Wiley books (Software Assessment: Reliability, Safety, and Testability [1995] and Software Fault Injection: Inoculating Software Against Errors [1998]. He received two U.S. patents and has over 250 publications. Voas received his undergraduate degree in computer engineering from Tulane University (1985), and received his M.S. and Ph.D. in computer science from the College of William and Mary (1986, 1990 respectively). Voas is a Fellow of the Institute of Electrical and Electronics Engineers (IEEE), the Institution of Engineering and Technology (IET), and the American Association for the Advancement of Science (AAAS).Voas's current research interests include software certification and the underlying science of IoT He is an IEEE Fellow.