Internet of Things and Radio Frequency Identification in care taking, facts and privacy challenges

Ines Frederix
Medical Doctor bachelor studies
University of Hasselt
Diepenbeek, Belgium
ines.frederix@student.uhasselt.be

Abstract— **Internet of Things technologies such as radio frequency identification are about to be able to help aging and sick people and even compensate for some disabilities. The use of these technologies in health care represents a promising development in information technology, but also raises important ethical, legal and social issues. This paper explores the use of these technologies in health care environments and formulates recommendations for further research that can ensure that the patients' privacy and dignity is preserved.**

Artificial intelligence, Communication system security, Identification of persons, Internet, Knowledge representation

I. Introduction

In the first week of my interimship in January 2009 at the neurologic and locomotoric revalidation centre it was very peculiar that some of the patients did wear a bracelet that in a mysterious way informed caregivers when the patient left a safe zone of the hospital.

My very first question had a simple answer. The bracelet was a radio frequency identification device (RFID) [10] that could identify the patient remotely. The two main types of RFID tags are passive and active. Passive tags contain no internal power supply. They convert the radio frequency energy emitted by a reader device into signals that transmit stored data for a distance of a few feet. These passive devices currently have restricted amounts of data storage and are of limited functionality but can work for years because they never run out of power. In comparison, active RFID tags contain an internal battery, which provides increased reliability, longer transmission ranges, on-tag data processing and greater data storage [2]. More advanced devices can combine RFID functionality with sensors to monitor health conditions of patients (e.g. in body measurement of glucose levels). Future devices will combine sensor functionalities with actuators and also exercise control functions (e.g. automated insulin injections by in body RFID actuators).

Also the second question, why the bracelet was used had a simple answer. It was an easy and efficient way to control the movements of the patient. Patients that for mental or physical conditions could not be left alone in the revalidation center received such a bracelet. Initially it was shocking to observe a patient that really was restricted in freedom due to the bracelet hadn't disappeared. This manuscript tries to indicate part of an answer on my remaining questions: How successful is the use of Internet of Things (IoT) technologies, such as RFID, WiFi, wireless sensor and actuators in health care today? How can it be ensured that personal information of the patient would not fall in the hands of strangers? Is the use of this technology compliant with European data protection legislation? Will the deployment of technology raise ethical questions?

II. IoT in outside health care

This section illustrates in a qualitative way that Internet of Things (IoT) type of applications hold the potential to revolutionize health care for patients that do not reside in a health care institute. The 3 described cases are examples of such applications.

A. The home patient

The world population is rapidly ageing: the number of people aged 60 and over as a proportion of the global population will double from 11% in 2006 to 22% by 2050. By then, there will be more old people than children (aged 0-14 years) in the population for the first time in human history. [1]

Internet of Things type of applications can improve the living conditions of these older people and allow them to stay longer independent and residential. This poses, however, various challenges related to privacy, respect for liberty, dignity and autonomy.

Applications that appear already on a large scale are monitoring systems such as sensors in exit doors that give warnings about undesired "movements", or devices that make it possible to localize elderly. These new applications mark the need for solutions that protect senior citizens from ethical and privacy risks as a result of misuse and abuse of these IoT applications.

The use of a device to track patients' movements to determine a sickness condition such as Alzheimer is already seen as too privacy invasive by some medical doctors [15] [16].

B. The nomadic patient

Future IoT applications using sensing technologies will be able to do real time monitoring of patients. Parameters such as blood pressure, glucose levels, heart and breathing rate … can be measured by lightweight devices worn by the patient without interference with daily activities. These wearable networked monitoring systems will be able to acquire, process and transmit data on multiple health parameters, letting medical professionals make better informed decisions without holding the patient in a hospital for observation. Medical staff will be informed in real time about any deterioration in patients' condition that triggers a need for intervention.

It is clear that this fundamental health information belongs to the strict privacy domain of the patient.

C. The tagged patient

The US Food and Drug Administration (FDA) approved in October 2004 the first passive RFID tags specifically intended for human implantation.

Human-implanted passive RFID devices that identify patients can also contain essential biometric and medical information. The tags are primarily intended for patients with chronic diseases, such as coronary artery disease, chronic obstructive pulmonary disease, diabetes mellitus, stroke or seizure disorder, or are implanted into patients with medical devices such as pacemakers, stents, or joint replacements. These devices have the size of a grain of rice, and can be implanted under the skin via a hypodermic-type needle.

The implanted RFID devices provide an efficient access to crucial data for patients but this fundamental health information belongs also to the strict privacy domain of the patient.

III. THE USE OF IOT AND RFID IN HOSPITALS

In fact, much is happening in health care ranging from IoT applications to streamline paperwork and business processes to advanced clinical applications to drive medical innovations—far too numerous to catalogue [3]. The applications can target an improvement in the quality of health care, or the processing of information, or increase the access to health care for patients and reduce the cost of the services.

One comprehensive study on the use of RFID in health care in hospitals was published recently on the web by Rand Europe [4]. They used a total of 325 sources to compile the report.

The study classifies the use of RFID in applications for assets, staff and patients. The table below taken from the Rand report and summarized in Figure 1 illustrates why patients receive sometimes an RFID tag:

1. Tracking (152 references):
   a. Patient tracking and tracing at hospitals to monitor the patient flow (55)
   b. Monitoring/tracking of patient location (38)
   c. Infant tracking and tracing at hospitals for security/to forego theft (16)
   d. Patient tracking to ensure safety/access control (12)
   e. Dementia patients tracking and tracing (11)
   f. Tracking of drugs, supplies and procedures performed on each patient (11)
   g. Real-time patient location systems (4)
   h. Accounting patient time in emergency department (3)
   i. Managing the large numbers of injured patients during catastrophic events (2)
2. Identification and authentication (220 references)
   a. Patient identification to reduce harmful incidents (112)
   b. Patient identification to avoid wrong drug, dose, time, procedure (51)
   c. Eliminate wrong patient/wrong surgery (30)
   d. Accurate patient identification for medication (13)
   e. Patient identification for blood transfusion (10)
   f. Reduce errors due to misidentification (7)
   g. Reduce patient complications (1)
   h. Portable, current and comprehensive health records (25)
   i. Critical information to the patient (11)
   j. Real-time clinical info associated with patient (5)
   k. Keeping current and comprehensive patient charts (5)
   l. Portable health records (3)
   m. Validating patient charts and imaging (1)
   n. Accurate patient identification (35)
   o. Implanted RFID carrying medical record (20)
   p. Infant identification to forego mismatching (12)
   q. Patient identification at disasters (8)
   r. Protecting patient privacy (3)
   s. Person identification for forensics (2)
   t. Contactless retail payment (2)
   u. Selectively jam RFID readers (1)
3. Automatic data collection & transfer (31 references)
   a. Interventions: automated care, pathways, procedures audit, management (23)
   b. Improving patient/staff satisfaction (6)
   c. Incident audit trail (2)
4. Sensing (52 references)

a. RFID ingested or implanted to provide real-time information on health indicators and vital signs, to monitor and report on the results of surgeries, to regulate the release of medications, telemedicine (22)

b. Intelligent medication monitoring (elderly at home) (15)

c. Assisting the visually impaired (4)

d. Infection control (nosocomial infections) (2)

e. Proper positioning of the endotracheal tube during intubation (2)

f. Clinical improvements (2)

g. Helping surgical recovery (2)

h. Tracking healing around an implant (1)

i. Functional-neuromuscular stimulation (1)

j. Flexible surface wetness sensor for adult paralyzed patients (1)

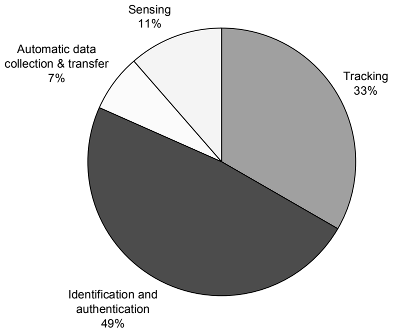

Figure 1: RFID use on patients in hospitals

A. Better healthcare delivery

According to the literature review made by the Rand staff in the report [4], the primary enabler for the use of RFID in healthcare delivery is the improvement in the quality of care associated with its implementation and near-term capabilities. These include the capacity to: reduce harmful incidents; improve the use of resources; deliver safe and fast unambiguous identification; and create an operationally-integrated hospital information system.

Some of the anticipated near-term RFID advantages have to do with: distant patient management (at home); biometric data collection; telemetry and intelligent out of hospital patient care.

B. Privacy, security, data integrity and ethical issues

The report [4] finds further that privacy, security, data integrity and ethical issues together form the largest barrier to wide-scale healthcare RFID implementations. The report cites also Sotto [5] who concludes that the benefits of RFID in medical settings are only achievable if patients are confident that the acquired data transmitted will not be misused. In addition, patients need to have confidence both in the security of the technology and in the related policy environment.

According to the reviewed sources, an additional set of obstacles to wider RFID implementation in healthcare are the cultural and ethical concerns associated with RFID.

IV. Internet of Things and Privacy

Internet of Things health related applications inside hospitals and outside can create privacy, security and ethical risks.

A. Privacy and data protection in care institutes

In health care institutes often the approach is to consider the use of the technology in the interest of the patient. First counts the health condition and by entering the care institute, hospital, elderly care, revalidation center… the patient gives consent to the use of such applications.

This simple interpretation today often found in these institutes does not consider some of the basic rights of the European citizens as described in the data protection directive of 1995 [6]. The hospital should not collect information of the patient that it does not need for the health care service nor keep the collected information any longer then strictly needed for the service it provides.

Hospitals are also semi-open environments, visitors can enter the facility and this creates additional privacy and security requirements. This can be illustrated on the hand of an example: Some early applications found in literature describe systems that monitor the location of patients at any time and display this location on large LCD displays. These systems have the advantage that doctors, specialists and medical staff can better plan the use of the often very expensive diagnostic equipment. But because the hospital is open for visitors the information on the LCD display can also be seen by visitors who by no means should have access to this information.

Sometimes, even when no data protection issues exist the application can be found to be too privacy invasive and criticized as non-ethical. An example of such an application can be found in another semi-open environment, airports. The 6th framework funded research project OPTAG [7] did develop an interesting application by combining a real time panoramic imaging system based on video cameras found in many public places with a long range radio frequency tagging system. This project succeeded to do a real time monitoring of passengers carrying RFID tagged boarding passes within an airport environment. The OPTAG system provides many advantages for the airport operator: checked in passengers who are either missing or late can be localized and passenger-induced delays in take-off reduced. It also provides a much higher airport security, not unimportant in the post September 11 era. Although very successful as project it had negative press coverage as too privacy invasive and also triggered questions and interventions at the European parliament. [8] Summarized can be said that the information revealed about travellers during their stay at the airport using OPTAG was seen as taking away the basic right of a person on privacy – even when at airports.

Care should be taken that in hospitals, elderly homes, revalidation centers …, the basic rights of patients on privacy are respected.

B. Privacy and data protection for outside care institutes

The problem will be more prominent in future applications that ensure health care outside care institutions. Sophisticated Internet of Things applications will help the senior to stay longer in his or her known home environment. These applications will make this possible by monitoring the movement of the senior in his house, protecting the senior against health risks (e.g. temperature of the water in the bad, time in bed,…) and audio-video contact. But even when the elderly person gives consent that a care taker and/or a close relative has access to this system it can also be considered as very privacy invasive, possibly taking away the privacy and dignity of the person. Without doubt sometimes the senior would like to be able to switch off the system.

C. Privacy and data protection for the nomadic patient

When the senior becomes a nomadic patient and not only a visual and/or geo-location monitoring takes place but also body parameters such as blood pressure, heart beat … are recorded the system becomes even more privacy invasive. These developments are seen by some as even going beyond the science fiction described by George Orwell in his famous work [9].

The new sensors and tags are so small that they can be implanted in the body. This can be done to have crucial data such as health records available, to make medication such a glucose level monitoring and insulin dosage convenient. But it can also be done to avoid tampering with the system. As an example implanted tags can serve to ensure that a tagged patient stays in a predefined zone, that health records are available to medical staff ... .

Privacy activists such as Dr. Katerine Albrecht (Harvard) started to condemn the use of such a technology, because of privacy invasiveness, by making a parallel to a story found in Christian literature "the mark of the beast" more then 2000 years ago. "*Time will come when people will carry a mark, the mark of the beast (devil) that will discriminate those that have the mark from those that have not*". Ms. Albrecht reworked the story in one of her books and uses it sometimes at some of the lectures she has given on the subject [11]. But she is not the only authority in the domain that warns for the privacy and ethical risks of such technological solutions.

V. PRIVACY FRIENDLY IOT APPLICATIONS?

From the preceding analysis it can be concluded that the Internet of Things and RFID creates a lot of opportunities to increase the quality of health care, to increase the convenience for the patient, to give him or her the option to stay longer at home, to reduce the time spent in hospitals for observation, to increase the diagnostic and treatment facilities available for caretakers, to give the patient a better treatment (exact glucose level control for diabetic patients …), and this at a lower cost.

But, literature shows, and this has been confirmed by a systematic survey of 325 pilot projects, that privacy and ethical risks are high and the most important inhibitor to proceed to a wider adoption of the technology.

The question remains what will happen when the hypothesis is put forward that no consideration is given to the concerns of ethical acceptable applications that respect privacy and dignity of patients ? Although not much is known for applications of this kind an analogy can be found in culture and psychology.

An arbitrary example that explains what can happen is the treatment of breast cancer by women. Each medical doctor will explain that preventive examination and timely treatment are essential to increase the survival rate for women. Several studies illustrate mortality rates that are much higher for some cultures such as Moslim women, or Chinese women that see an illness as a fate that they have to fight alone. A more quantitative result has been obtained by the US cancer institute [12] that came to the conclusion that in the US the chance to survive breast cancer for white women is 30% higher than for black women. They came to this result after removing all the factors that could deliver another explanation such as age of the patient, place of living…. The main finding was that the difference in culture, less concern of black women for their health, is the main reason for late diagnosis and explains the lower chance for survival.

For the use of new Internet of Things technologies in health care this finding is also important. If these applications do not cover privacy concerns of the patients the risk exist that some patients concerned with their privacy and dignity will not use the possibilities of advanced home care, the nomadic patient … leading to a lower quality of health care for these patients.

The conclusion is that privacy and data protection characteristics are crucial for such applications. How this can be ensured has been a subject of an extensive public debate of the last years [13].

A. Legislation

Law has his merits and is an effective means to protect the privacy and ethical rights of the patients. The European Union has a set of Directives, or European laws, of which the data protection Directive 95/46/EC [6] is the most important one to protect the rights of its citizens.

This legal framework is an instrument to teach what the essential data protection and security constraints are of such applications and provides the means to fight unlawful behavior that would jeopardize the privacy of European citizens and patients. The legal framework has however at least two limitations: (1) it can not cover the fast technological developments in the domain and (2) the enforcement of legal rules is a time and resource consuming process and often comes too late for the victims of "privacy violations".

B. Security in the system

Privacy and security should be embedded in health applications to minimize the risk for the patients. Research for privacy enhancing solutions is needed for these applications. The industry has already recognized this need and started investments in technologies such as encryption to ensure that information can not leak easily in the wrong hands. The European Commission welcomes such initiatives and released recently a communication on the importance of privacy enhancing technologies [14].

C. Behavioral modeling in the system

Surprisingly enough, within the many publications in the domain, not much can be found on the importance to invest in knowledge engineering technologies to ensure privacy and dignity of patients.

In home care application scenarios it is clear that caretakers need to have access to much information to help a patient when needed. Even when the patient has given consent this sometimes can be embarrassing.

To avoid these issues Internet of Things applications for home care or the nomadic patient should be able to execute patient monitoring and to decide, using artificial intelligence techniques, if a patient behavior could be qualified as strange and possibly endangering his/her health triggering the need for assistance from health care professionals. Besides the fact that much less information is shared with care takers it makes the application also much more efficient: Care takers receive a call only when reasons exist to be worried about the patient.

VI. Conclusion

The manuscript illustrated how RFID is used today in pilot applications in hospitals and predicts Internet of Things application scenarios for healthcare in the future. Based on literature studies it concludes that many of these application scenarios are strongly privacy invasive. The short analysis concludes that more investment in privacy enhancing technologies is needed to ensure acceptance of the applications by the patients. It also identifies, and this is the most important conclusion, artificial intelligence and knowledge management research as important means to ensure that the privacy and dignity of patients, especially in outside health care and nomadic patient applications is respected.

Acknowledgment

The author would like to thank the European Commission for making so much information on RFID and the Internet of Things online available.

References

[1] E. Mordini, "*Social, Ethical and Privacy needs in ICT for older people*", EU funded Seniorproject, Center for Science, Society and Citizenship 2008. Available: www.seniorproject.eu

[2] K. Mun, SK Mun, "RFID in Healthcare: The Applications, and Obstacles, Are Many"; *Journal of AHIMA*, Volume 77(8): pp. 56-62, 2006.

[3] R. D. Atkinson, D. D. Castro, "*Digital Quality of Life. Understanding the Personal & Social Benefits of the Information Technology Revolution,*", The information & Technology innovation foundation, pp. 25-27, 10/2008 Available: http://www.itif.org/index.php?id=34

[4] A-M. Vilamovska, E. Hattziandreu, R. Schindler , C. van Oranje, H. de Vries and J. Krapelse, "*RFID application in healthcare - Scoping and identifying areas for RFID deployment in healthcare delivery*", Rand Europe, July 2008 Available: http://ec.europa.eu/information_society/activities/health/docs/studies/200807-rfid-ehealth.pdf

[5] Sotto, J. Lisa, "*Testimony on Privacy Issues Associated with the use of RFID Technology in Health Care Setting*", Hunton & Williams LLP, 2008.

[6] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal of the European Communities of 23 November 1995 No L. 281 p. 31. Available: http://www.cdt.org/privacy/eudirective/EU_Directive_.html

[7] S. Robson, G. Gyory, "*OPTAG - A combined panoramic photogrammetric and radio frequency tagging system for monitoring passenger movements in airports*", Department of Geomatic Engineering, UCL, Gower Street, London, (2004 – 2007) Available: http://www.isprs.org/commission5/proceedings06/paper/1262_Dresden06.pdf

[8] S. In't Veld, "*Worrying developments in airline data privacy need closer scrutiny*", Member of the European Parliament, (2007) Available: http://www.alde.eu/en/details/news/worrying-developments-in-airline-data-privacy-need-closer-scrutiny/

[9] G. Orwell, E. Fromm, "*1984: a novel*", Signet Classic, 1990. Available: http://books.google.com/books?id=yxv1LK5gyV4C

[10] "*Radio-frequency identification, a comprehensive overview*". Available: http://en.wikipedia.org/wiki/Radio-frequency_identification

[11] HL. Ward, "*Microchip Implants Raise Privacy Concern; Submit To Chip Implant Or Lose Your Job?*", 2007. Available: http://newsgroups.derkeiler.com/Archive/Alt/alt.privacy/2007-07/msg00054.html

[12] US National Cancer Institute study on breast cancer, Surveillance Epidemiology and End Results – cancer statistics, 2008 Available: http://seer.cancer.gov/statfacts/html/breast.html

[13] Information Society and Media directorate general, SEC (2007) 312, "*Results of the public online consultation on future radio frequency identification technology policy*" Available: http://ec.europa.eu/information_society/policy/rfid/documents/rfidswp_en.pdf

[14] European Commission, Justice, liberty and security directorate general, "*Working documents on privacy enhancing technologies*" Available:http://ec.europa.eu/justice_home/fsj/privacy/studies/priv-enhancing_en.htm

[15] K. Grifantini, "*Wireless Detectors for Dementia,*" *MIT Technology review*, Feb. 2009 Available: http://www.technologyreview.com/computing/22043/page1/

[16] C. Macdonald, "*Is Behaviour Tracking Minimally Invasive?*", *The research ethics blog*, Available: http://www.researchethics.ca/blog/2009/02/is-behaviour-tracking-minimally.html