Transforming Healthcare with the Internet of Things
J. Hofdijk et al. (Eds.)

doi:10.3233/978-1-61499-633-0-46

Non-technical Issues in Design and Development of Personal Portable Devices

Lenka LHOTSKA [a,1], Paul CHESHIRE [b], Peter PHAROW [c], and David MACKU [a]
[a] *Czech Technical University in Prague, Czech Republic*
[b] *Independent Consultant, Kent, United Kingdom*
[c] *Fraunhofer Institute for Digital Media Technology IDMT, Ilmenau, Germany*

Abstract. Mobile technologies are constantly evolving and with the development of Internet of Things we can expect continuous increase of various applications. Mobile technologies have undeniable opportunities to play an important role in health services. Concerning purely technical aspects, almost every problem can be solved. However, there are still many unsolved and unclear issues related with ethics and governance mechanisms for mobile phone applications. These issues are even more critical in medical and health care applications of mobile technologies. This paper tries to analyse ethical, and privacy-related challenges that may occur when introducing Personal Portable Devices (PPD) to collect and record personal health data in health care and welfare environment.

Keywords. Personal Portable Devices, Ethics, Human Factors

Introduction

The integration of mobile technologies, sensors, sensor networks and portable devices to provide personal services of many kinds, especially those involving location tracking or lifestyle and well-being, will require wide acceptance of these technologies by ordinary citizens. When we design and develop applications for health care and welfare, we have to consider users related issues much more carefully than in other more general applications. Recently, at many conferences and in many journal articles, various technological issues concerning Personal Portable Devices (PPDs) have been discussed and many new solutions have been proposed. With the advent of Internet of Things and their applications in health and social care, the requirement of wide acceptance is becoming more urgent. However, the non-technical dimensions of the applications remain almost unnoticed. Whilst it is clear that many portable technologies are widely used by people of all ages and abilities, their field of application is more "recreational" than "clinical". Without giving adequate consideration to psychological, ethical and legal issues it would be very difficult to introduce any technological solution that supports or replaces healthcare professionals into routine use. In this paper we try to identify and discuss the most important problems that should be solved (at least to some extent) before portable "clinical" technology is planned to be introduced to the market.

Since it is assumed that these systems will be mostly used by people who are not technology specialists (care givers, patients, their families, social workers, etc.) it is

[1] Corresponding Author.

necessary to focus even more on: the acceptability of these devices by everyone in the chain of care, human-computer interaction, easy and intuitive control, prevention of misuse, etc. In addition to these items, there are many questions linked with data collecting, storing, processing, access, and use. We try to analyse the major legal and ethical issues which arise from the handling of sensitive data about health and data about everyday activity patterns. Since the space is limited we focus on ethical issues in relation to different modes of use of personal portable devices and mobile applications.

1. Methods

In our research we decided to analyse the management of ethical issues connected with mobile technologies and PPDs in different applications and different settings. We tried to report quantitative information about the growth of number of users and applications advocating the importance of development of a certain regulatory framework. When relevant, we mention existing legal regulations or guidelines. It is necessary to distinguish for which purpose the mobile technologies and PPDs are used, who interprets the acquired data and how the patient is informed about his/her state. From the regulatory point of view there is rather strict division of applications for medical purposes on one side and fitness and well-being on the other side.

Mobile technologies evolve constantly and with the advance of Internet of Things we can expect continuous increase of applications installed in persons´ homes, senior homes as well as an increase use of wearable's for measurement of vital parameters and behaviour monitoring. Since 2007 we observe continuous growth of mobile devices. Number of mobile phone users has increased from 400 mil. users in 2007 up to almost 2 bil. in 2015. It is expected that by 2017 the global coverage by commercial wireless signal will reach 85% of the world´s population [1] and approximately 3.4 bil. people worldwide will own a smartphone. Half of them will use health apps.

However, there are still many unsolved and unclear issues concerning ethics and governance mechanisms for virtual technology and for mobile phone applications. In this respect, a significant change happened in September 2013, when the FDA released guidance for the developers of mobile medical apps [2]. „Mobile medical apps" are defined as applications which are intended „to be used as an accessory to a regulated medical device" or „to transform a mobile platform into as regulated medical device ".

In the EU, there are no binding rules as to the delimitation between lifestyle and wellbeing apps and a medical device or in vitro diagnostic medical device. As the use of these apps is affected by existing EU regulatory instruments, stakeholders, such as mobile app developers and mobile platform manufacturers, may seek guidance as to the applicable rules. Since January 2012, in order to help software developers and manufacturers to identify whether their products fall or not under the Medical Devices Directive (Directive 93/42/EEC on medical devices, OJ L169,12.07.1993) or the in vitro diagnostic medical devices Directive (Directive 98/79/EC on in vitro diagnostic medical devices, OJ L331, 7.02.1998) [3], the Commission's services have issued some guidance on this issue, which will be continuously updated. According to this guidance, depending on their intended purpose, apps may fall under the definitions of a medical device or of an in vitro diagnostic medical device and consequently will have to comply with the relevant provisions of the aforementioned directives. Since this delimitation is not yet clarified through binding rules, when the Medical Devices Directives do not apply to apps, clarity is required as to the rules with which they must comply. The fact, that Union

legislation could not yet address latest developments in this sector and that the Court has not had the opportunity to clarify the applicability of existing legislation on these newly developed apps, still leaves room for interpretation. Thus in April 2014, the European Commission launched a public consultation alongside the Green Paper on mobile health (mHealth) [4] to help identify the right way forward to unlock the potential of mobile health in the EU. Together with the Green Paper, the Commission also published a Staff Working Document on the existing EU legal framework applicable to lifestyle and wellbeing apps [5], providing legal guidance on EU legislation in the field to app developers, medical device manufacturers, digital distribution platforms, etc.

In the world there are over 150 countries that have to develop any kind of regulatory framework for apps. It will be a complex process because it is impossible to apply one model of mHealth solution to all these countries. The reason is that every country has a unique health system with its own legal regulations, which these apps must fit with. However, even existence of guidelines and a framework does not guarantee quality of the apps as findings in [6] illustrate. The study published in the New England Journal of Medicine in 2014 shows that in the USA only about 100 of 100 000 health care apps are FDA approved. Many of the apps are used for collecting and analysing data from basic wearable's, whose market is also continuously growing. In [7] FierceMarket informs that while in 2014 26.4 mil. basic wearable's (such as fitness wristbands) were shipped, in 2015 the number significantly increased to 72.1 mil. Therefore, the importance of validation of the apps becomes more pronounced.

2. Results

Based on the analysis and our practical experience we identified several groups of applications that differ by their purposes. The first group aimed at clinical research uses the collected data in controlled manner might be purely software app or combination of a medical device and software. The data are interpreted and verified by medical experts. The second group utilizing purely mobile applications developed in frame of clinical research and transferred to routine use collects data from the patients. The data are sent for interpretation to a medical centre. The third group, aimed at general population, can be either mobile apps in smart phones or applications collecting data from, for example, fitness wristband. Regarding output of the applications, the first two groups might represent decision support systems, while the last group represents recommender system [8]. In all cases the data are transmitted: from device to mobile phone and then to a medical centre. Although data privacy and security are well defined and the technological tools are well developed there are many problems and insufficiencies in existing applications. Recent study [9] revealed failures even in certified apps. Another issue which we did not find in any source is data persistence in mobile apps. For long-term monitoring of health state, we want to have access to past data. What happens when the user changes the type of the smart phone, brand or operating system? Is there any chance to transfer the stored data in format readable on the new device?

The major ethical issues arise from the handling of sensitive data about health and daily activities. Explicit informed consent must be obtained from the participants in order to include this sensitive data in their Electronic Health Record (EHR) or on local storage. They must also consent to their data being shared, transmitted and analysed by authorized personnel within the designed system. In mobile apps it is sometimes not clear who might have access to the data or where the data are sent.

All the procedures must conform to relevant EU legislation (in EU countries) and to national legislations related to the principle of respecting confidentiality. Let us consider a case of cross-border utilization of the system and data communication between two EU countries. The applications must be compliant with legal frameworks of both countries. Even in EU the situation is not that simple. Although it exists EU directives, the national legal regulations usually have some additional restrictions or requirements. A good example is data privacy. For example: Czech law does not explicitly state where the data should be physically stored. The only requirement is that the person/institution that collects such data ensures technical and organizational measures for data security and privacy. Spanish law puts additional requirements on the technical side and defines where and under which measures the data should be stored.

When designing any system that collects patient data all subjects must participate voluntarily after being informed of the objectives and methodologies of the project. Explicit written consent will be requested. Since some difference in respecting privacy could arise between different subjects, two different forms for informed consent / authorization should be used: 1) subjects who will authorize use of personal data; 2) physicians who consent to use their information and knowledge about patients who already agreed to participate. To be enrolled, both consents are needed.

All the researchers involved who take part in the analysis of non-anonymous data must be asked for an explicit declaration of respecting confidentiality. Personal data must not be used for commercial purposes. In the management of sensitive data, it is necessary to define proper levels of security. In most cases it is essential to assure both secure transmissions and secure storage and management of data and knowledge. Concerning development of an application, the following questions must be answered: Will be the behaviour of the patient recorded? Who will have access to the data? How long should the data be stored? Will the data be stored locally or in a central data storage? Are there any national legal regulations concerning the domain? How can the legal regulations influence the technological design and use of the proposed system?

Legal clarity, or rather the lack thereof, is a key issue. The lack of a clearly set out legal framework, in particular with regard to licencing, accreditation and registration of telemedicine, assistive technologies and ambient assisted living services and professionals, liability, reimbursement, jurisdiction, is a major challenge.

3. Discussion

Activities in medical areas are well reflected in ethical and legal documents. Thus the part of AAL handling data about persons' health state can be approached in the same way. However, the daily activities monitoring and other activities must be described appropriately with respect to ethical and legal frameworks valid in corresponding countries. Recently we have identified certain gaps in legal regulations on the border between health and social care in some countries with regard to application of mobile technologies, assistive technologies and currently Internet of Things (IoT). The critical issue as we see it from discussions at national level is data privacy, in particular who can have access to which part of patient/client data and how detailed information should be stored locally or globally and how long.

As we have already mentioned there are differences among EU countries in legal regulations. In addition, there are also differences in organization of health and social care. For example, in Austria both types of care are under the umbrella of one ministry;

in the Czech Republic health care is under the responsibility of the Ministry of Health and social care is controlled by the Ministry of Labour and Social Affairs. Thus the processes describing care provision are definitely different. This issue must be considered during the design and development of the applications. It will also influence processes necessary for cross-border provision of health care. Obviously in the future utilization of mobile apps across borders will be demanded more and more. However, the procedures are not clearly defined yet. Benefits of these apps will depend on how they are treated in the social context of the countries in which they are used. Wireless networks transcend borders, but not every country has the same health system and health care policy. Easier operation will probably lead to a requirement of certain process interoperability definition.

Acknowledgement

The authors are indebted to the EFMI WG PPD members, and to all supporters of the WG PPD work in past and present. Research of Lenka Lhotska has been supported by the AZV MZ CR project No. 15-25710A “Individual dynamics of glycaemia excursions identification in diabetic patients to improve self-managing procedures influencing insulin dosage” and research of David Macku has been supported by CVUT institutional resources (SGS grant application No. OHK3-033/16).

References

[1] Savitz E. Ericsson: 85% global 3G coverage by 2017; 50% for 4G. *Forbes*. 6 May 2012. http://www.forbes.com/sites/ericsavitz/2012/06/05/ericsson-sees-85-global-3g-wireless-coverage-by-2017-50-4g-coverage/ (accessed 12 October 2014).

[2] U.S. Food and Drug Administration. *Mobile medical applications: guidance for industry and Food and Drug Administration staff.* U.S Department of Health and Human Services. 2013.http://www.fda.gov/downloads/MedicalDevices/…/UCM263366.pdf

[3] EU law and other EU public documents (online) retrieved on 26-10-2015 from http://eur-lex.europa.eu/homepage.html

[4] GREEN PAPER on mobile Health ("mHealth") Brussels, 10.4.2014 COM(2014) 219 final {SWD(2014) 135 final} (online) retrieved on 10-02-2016 from https://ec.europa.eu/digital-agenda/en/news/green-paper-mobile-health-mhealth

[5] COMMISSION STAFF WORKING DOCUMENT on the existing EU legal framework applicable to lifestyle and wellbeing apps Accompanying the document GREEN PAPER on mobile Health ("mHealth") Brussels, 10.4.2014 SWD(2014) 135 final {COM(2014) 219 final} (online) retrieved on 10-02-2016 from https://ec.europa.eu/digital-agenda/en/news/commission-staff-working-document-existing-eu-legal-framework-applicable-lifestyle-and

[6] Cortez NG, Cohen IG, Kesselheim AS. FDA regulation of mobile health technologies. *N Engl J Med*2014;371:372-9.

[7] http://www.fiercemobilehealthcare.com/story/why-security-must-be-top-focus-mhealth-wearable-data-exchange-strategy/2015-06-27

[8] Pharow, P. - Lhotská, L. - Cheshire, P.: Personal Portable Devices as Enablers for Advanced pHealth Decision Support and Decision Making Services. In *Proc of the 10th Int Conference on Wearable Micro and Nano Technologies for Personalized Health*. Amsterdam: IOS Press, 2013, p. 27-32.

[9] K. Huckvale, JT Prieto, M Tilney, PJ Benghozi, and J Car. Unaddressed privacy risks in accredited health and wellness apps: a cross-sectional systematic assessment. *BMC Medicine* (2015) 13:214