A roadmap for future human-machine networks in eHealth

Eva Jaho, Marina Klitsi, Nikos Sarris

Innovation Lab

Athens Technology Center

10, Rizariou str, 152 33 Halandri, Athens, Greece

{e.jaho, m.klitsi, n.sarris}@atc.gr

1 Introduction

The advancements in micro/nano-, bio-technology, data management and telecommunications are revolutionizing the provision of healthcare services worldwide. Healthcare services assisted by telecommunications and electronic equipment, also known as eHealth services, include Electronic Health Records (EHRs), telemedicine networks and applications (including telesurgery) and networks for physiological monitoring of patients with smart mobile or wearable devices. Assisted by technological developments, the healthcare community is moving toward early detection of diseases, health status monitoring, healthy lifestyle, and overall quality of life (Lymberis & Dittmar, 2007). Today, there are devices and applications for the management of chronic diseases, back problems, biochemical indices, heart problems, and many other medical conditions. Such personalized eHealth services can benefit the entire community by improving access to care, quality of care and by making the health sector more efficient.

The interaction of humans and machines for the provision of healthcare services poses several challenges: quality provisioning, the efficient management and protection of personal medical data, and the economic and social sustainability of the services. Higher machine agency in a domain were human relationships were traditionally predominant necessitates the establishment of human trust in machine operation and capabilities. Moreover, for a massive uptake of such services it is essential to motivate people for behavioural changes, and make the services affordable at low cost.

In this short paper, we provide an overview of the challenges and envisaged actions at European level for the efficient integration of personalized eHealth systems, devices and applications in human life and societies. The study is based on the **Roadmap for *eHealth Human-Machine Networks (HMNs)***, which was developed in the course of the HUMANE project.[1]

2 Policy background and regulatory context

According to EC's action plan on eHealth for 2012-2020[2], one of the barriers to the development of eHealth is the lack of clarity on legal and other issues around mobile health ("mHealth") and "health & wellbeing applications" and about the role that network operators, equipment suppliers, software developers and healthcare professionals could play in the value chain for mHealth.

In April 2014, the European Commission published a Green Paper on mHealth[3], which explored the potential of mHealth, and issues such as privacy, patient safety, legal frameworks and cost-effectiveness. 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, providing legal guidance to app developers, medical device manufacturers, digital distribution platforms, etc.[4] Following these works, the EC planned to establish an industry-led Code of Conduct for mobile

[1] HUMANE: a typology, method and roadmap for HUman-MAchine NEtworks (Project number: 645043 - H2020-ICT-2014-1, https://humane2020.eu)

[2] European Commission. (2012). eHealth Action Plan 2012-2020 – Innovative healthcare for the 21st century.

[3] European Commission, "GREEN PAPER on mobile Health ("mHealth")". Brussels, 10.4.2014. Available online at: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=5147

[4] European Commission, "COMMISSION STAFF WORKING DOCUMENT on the existing EU legal framework applicable to lifestyle and well-being apps". Brussel, 10.4.2014. Available online at: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=5146

health apps, which was recently released[Error! Bookmark not defined.]. The objective of this code is to foster citizens' trust in mHealth apps, raise awareness and facilitate compliance with EU data protection rules for app developers. [5] Furthermore, in February 2016 the EC appointed a working group with the mission to draft mHealth assessment guidelines that could help different stakeholders, in particular end-users, in assessing the validity and reliability of mobile health applications.

3 eHealth HMNs implications

Personalized eHealth systems, devices and applications imply increased control and intervention by patients for the detection, treatment and management of diseases. While knowledge and activation on the part of patients used to be necessary for the management of chronic diseases such as diabetes and hypertension, patient activation and knowledgeability is now required for more sophisticated conditions, like heart problems, but predominantly for the monitoring of vital signs and the uptake of a healthier lifestyle, in order to prevent diseases. Therefore, eHealth HMNs need on the one hand to be designed so as to educate people for the handling of more complex health conditions, and to motivate otherwise healthy individuals to monitor their health conditions.

Basic implications for human activation in eHealth HMNs are the protection of privacy and confidentiality of medical information. This has to be ensured through efficient data management and security mechanisms, i.e. encryption and authentication mechanisms on all communicated data (sensor-to-sensor communication in a body area network or home network, or data communication from the home network to a hospital backend). Additionally, it is necessary to apply consistent rules in the EU for the management of medical information.[6]

Data protection rules are expected to tackle another challenge, that of increasing trust and mitigating resistance from the patients and healthcare providers in using such products. A user of an eHealth device or application should be aware of what happens to the data that are recorded and communicated. In addition, a user should be able to authorise the parties which are using the data, and the ways in which they are used. Design solutions should increase information towards users, so that they receive feedback on the actions performed, and are able track usage traces for the provided data. Additionally, a data management service could be offered that tracks data access attempts, as well as refuses data release without explicit consent and/or generic agreement.

Another facet of high machine agency in eHealth systems concerns the very large volumes of data produced, and the subsequent need for an efficient data management. The increased reliance on machines also calls for increased security and QoS guarantees in service provisioning. Non-availability of eHealth services may produce a major risk for patients' health. Additionally, avoidance of Internet traffic congestion becomes highly significant, especially for critical applications, such as remote heart monitors.

Security concerns the integrity of medical data and devices, and protection from threats like eavesdropping and denial of service. For example the EC, in its 2014 Green paper on mHealth,[3] noted the risks for accidental exposure of medical data to unauthorized parties, and the risks from loss or theft of devices storing sensitive information. They concluded that mHealth solutions should contain specific and suitable security safeguards such as the encryption of patient data and appropriate patient authentication mechanisms to mitigate security risks.

Finally, there have been numerous calls for standardization and interoperability of ICT platforms, methods and services for eHealth. This is related to global efforts for standardization of M2M communications. Currently, eHealth standardization is under active consideration in different standards fora such as ETSI TC M2M, ETSI TC e-Health, ITU-T Focus Group (FG) on M2M etc. Interoperability and standardization are also expected to create economies of scale that can provide more cost-efficient systems and services. There is a need for harmonizing the spectrum in which these devices operate across the whole of Europe and ideally, worldwide, as the Industrial

[5] https://ec.europa.eu/digital-single-market/en/news/mhealth-green-paper-next-steps

[6] A step in this direction is the patient data Privacy Code of Conduct on mobile health (mHealth) apps, mentioned in Section 2.

Scientific and Medical (ISM) band seems to be overcrowded. Barriers to standardization include the existence of proprietary systems, the massive amounts of data being collected from these systems, the lack of standard content format and the lack of open freely available standards (Fan, Haines, & Kulkarni, 2014).

4 Actions and future directions

Based on desk research and a series of interviews and workshops with different stakeholders (ICT experts and researchers in the eHealth domain, policy makers, professionals and patient groups), the HUMANE project has identified a series of actions to address HMN implications and facilitate the broader uptake of eHealth service in a way that is beneficial for society.

In order **to ensure the efficient management and protection of medical data** stored and communicated by eHealth monitoring devices, we consider that realistic large scale studies are required, which will systematically examine the application of advanced data management by eHealth HMNs. Besides efficient storage, categorization and search of eHealth data, the focus should be on real-time event detection, for early avoidance of severe health episodes. Different levels of detail should be provided depending on the intended use (e.g. raw data for use by medical researchers or aggregated data for statistical reports) and the level of authorization of the persons accessing the data.

Empowering users to manage their personal information, and to control the level of confidentiality needs an integrated approach of applying **privacy-by-design mechanisms** in commercial eHealth HMN. Similarly to data management, we consider that large-scale pilot studies of such systems would be extremely helpful. In addition, we should examine the application of the forthcoming mHealth code of practice and assess its efficacy. In addition, techniques should be demonstrated that empower the users to take control of their personal data, and provide transparency with regard to their exploitation by the data collectors and any third parties. The demonstrated systems should also be robust to attacks and eavesdropping, and have advanced encryption and authentication mechanisms.

To ensure the availability of critical eHealth services offered by monitoring devices in the public Internet, it is necessary to develop eHealth services with guaranteed QoS. Providing QoS guarantees in the public Internet is a longstanding problem existing for about 35 years, and failures to do so are attributed to a mixture of technical, business, and political reasons (kc claffy & Clark, 2015). Currently, the penetration of Internet services in everyday life, including critical human and societal functions, has refurbished the interest in this topic. There is increasing talk about 'specialized' or 'managed' services, or services 'other than Internet access services', as is the terminology in the recent European Open Internet Regulation (EU) 2015/2120. We believe that a concerted effort of the involved parties (ISPs, content providers, and consumers) is required to provide such services in practice without undermining the general quality of the Internet, and jeopardizing the benefits that Internet freedom and equality has brought to the public.

To ensure the interoperability of eHealth devices and data from such devices, it is necessary to harmonize the frequency band for the operation of such devices, and to encourage the development of standard content formats for the exchange of generated medical information. Other functions for which standards should be developed are the networking architecture, as well as the configuration of devices and reading of measurement data.

Regarding the need **to provide such systems at reasonable cost**, it is necessary to harvest the experience by offering products with eHealth monitoring capabilities in recent years. A study of existing business models is required that compares different models and forms of state subsidies, and also examines regulatory differences in each country, as well as differentiations based on the social conditions and mean income.

Regarding the **legal framework**, it is necessary to review and merge the provisions of the different regulatory documents that relate to eHealth HMN: the Data Protection Directive, the e-Privacy Directive, the Consumer's Rights Directive, the eCommerce Directive, and the Unfair Commercial

Practices Directive. It should aim at removing redundancies and resolving ambiguities in the marketing and use of eHealth HMN.

Finally, **clinical validations** should aim at deriving best practices and discovering the safest and most efficient monitoring systems, and at demonstrating the integration of eHealth HMN with current clinical practice procedures. Such practices could then become norms that such products should follow. To this end, there is also a need to collect the experience from clinical tests that have already been performed with eHealth monitoring devices.

The following figure shows the timeline for implementing the aforementioned actions, through a 10-year period. The standardization and interoperability of eHealth devices, as well as the provision of eHealth services with guaranteed QoS are considered as continuous tasks during the whole period. The periods for the remaining tasks have been estimated based on experience and the degree of difficulty of the tasks.

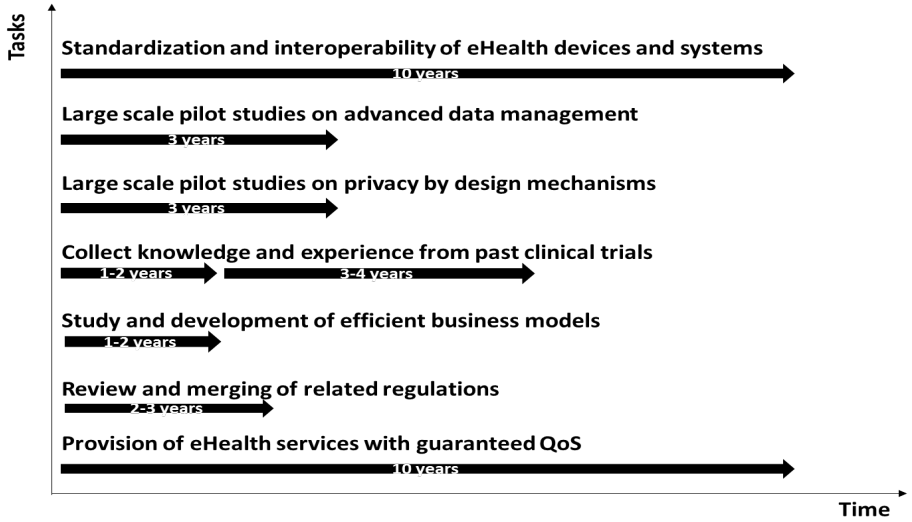

Figure 1: eHealth HMN timeline

More details and a description of stakeholder roles in implementing the above actions can be found in (Jaho et al., 2017)[7].

5 References

Fan, Z., Haines, R., & Kulkarni, P. (2014). M2M communications for E-health and smart grid: An industry and standard perspective. *IEEE Wireless Communications*, *21*(1), 62–69. http://doi.org/10.1109/MWC.2014.6757898

kc claffy, & Clark, D. D. (2015). Adding Enhanced Services to the Internet: Lessons from History. In *Proceedings of the 43rd Research Conference on Communication, Information and Internet Policy (TPRC'15)* (pp. 1–28). Retrieved from http://ssrn.com/abstract=2587262

Lymberis, a, & Dittmar, a. (2007). Advanced Wearable Health Systems and Applications - Research and Development Efforts in the European Union. *Engineering in Medicine and Biology Magazine, IEEE*, *26*(3), 29–33. http://doi.org/10.1109/MEMB.2007.364926

Jaho, E., Klitsi, M., Følstad, A., Lech, T. C., Walland, P., Pickering, J. B., & Meyer, E. T. (2017). *D4.4 Final roadmap of future human-machine networks*.

[7] The document will be made available on https://humane2020.eu/publications/ from July 2017. Prior to this, please contact e.jaho@atc.gr for an individual copy.