ESIP response to the public consultation of the European Commission on the GREEN PAPER on mobile Health ("mHealth")

- COM(2014)219 final

Submitted

03 July 2014

About the *European Social Insurance Platform* (ESIP)

The *European Social Insurance Platform* (ESIP) represents over 40 national statutory social insurance organisations (covering approximately 250 million citizens) in 16 EU Member States and Switzerland, active in the field of health insurance, pensions, occupational disease and accident insurance, disability and rehabilitation, family benefits and unemployment insurance. The aims of ESIP and its members are to preserve high profile social security for Europe, to reinforce solidarity-based social insurance systems and to maintain European social protection quality. ESIP builds strategic alliances for developing common positions to influence the European debate and is a consultation forum for the European institutions and other multinational bodies active in the field of social security.

Statement regarding positions submitted by ESIP: *ESIP members support this position in so far as the subject matter lies within their field of competence*. *ESIP's positions are not legally binding on its members.*

ESIP, rue d'Arlon 50, B – 1000 Brussels
Tel: +32 2 282 05 62; Fax: +32 2 282 05 98
Web: www.esip.org

Contact: christine.dawson@esip.eu

ESIP welcomes the opportunity to comment on the green paper on mobile Health ("mHealth") and to provide the European social insurers' perspective through the open public consultation.

ESIP supports the aim of the European Commission which is to analyse the potential benefits and problems faced in implementing mHealth services. The statutory health insurance (SHI) funds need to guarantee high quality health care for their insured citizens. Health insurers recognise the potential of mobile health apps and already today, compulsory health insurances offer a multiplicity of apps to citizens for patient consultation, education and information.

A key issue surrounding mobile health solutions is security, both as regards personal data protection and the functioning of the device and/or application. Basic requirements for secure processing of health data are end-to-end encryption, clear access rights and secure authentication of authorised users. The current EU data protection Directive is not sufficient in this regard.

Furthermore, it is important that mHealth apps which go beyond an aid to consultation, education and information are reliable and safe. Those apps designed for diagnosis, therapy or screening should be governed by the medical devices Directive 93/42 EEC (and any subsequent revision of this Directive) and should be authorised by the designated body to ensure the efficacy and functionality of the products.

Finally, it is important that conditions for mHealth solutions are improved throughout the European Union to develop their full potential without reducing existing levels of data protection.

3.1 Data protection, including security of health data

- Which specific security safeguards in mHealth solutions could help to prevent unnecessary and unauthorised processing of health data in an mHealth context? How could app developers best implement the principles of "data minimisation" and of "data protection by design", and "data protection by default" in mHealth apps?

  mHealth solutions should fully comply with EU legislation on data protection. Further, an independent certification body/authority should be established to ensure that any mHealth solution provides sufficient protection against unnecessary and unauthorized processing of health data. Common technical safeguards applied to many mHealth solutions should be extended to other mHealth scenarios. These include, but are not limited to, encryption, authentication and registration of devices. Special concern should be given to the latter, for example, where a patient's personal data is legally downloaded and used by a health care professional on his own device, but later "forgotten" and then remains on the device. A possible solution to this case scenario would be to use a cloud-based solution (SaaS), where the data can be accessed and used on health care professionals' private devices, but no actual data is stored on the device. However, the processing and storage of health data in cloud systems requires very strong data protection rules and stringent safety requirements.

The principles of data minimization should be implemented within mHealth apps using all the necessary tools (depending on the type of application). This refers to a selective approach on collecting, storing and processing personal data. For each of the healthcare processes covered in the mHealth services the developers should be vigilant not to request access (either from a centralised data source, such as electronic health records, or as user input) to data that is not necessary to provide the desired service to the patient. Regarding the principles of data protection by design & by default, both should be used, again depending on the process covered by the mHealth application. If in doubt, the preferred option is data protection by default, since this would protect most of the data (even if the patient is not aware of the need for protection).

3.2. Big data

- What measures are needed to fully realise the potential of mHealth generated "Big Data" in the EU whilst complying with legal and ethical requirements?

  In principle data minimisation and the appropriation of data should be considered. Only absolutely necessary data should be collected, generated and processed. National and EU authorities should ensure correct transposition of EU data protection rules.

  When processing personal health data it should be obligatory to inform insured persons and patients fully about the process, the risks and the benefits of processing their data.

3.3. State of play on the applicable EU legal framework

- Are safety and performance requirements of lifestyle and wellbeing apps adequately covered by the current EU legal framework? Is there a need to strengthen the enforcement of EU legislation applicable to mHealth by competent authorities and courts; if yes, why and how?

  ***Data protection**:*

  Due to the cross-border character of processing and use of health data, additional and unitised regulation is necessary. It has to be transparent for which purpose data will be collected and processed, when and whether they will be deleted when the app is uninstalled and where the data is recorded. The current European data protection Directive does not deal adequately with this issue.

  ***Authorisation of mobile health application**:*

  As some mobile applications will need to be considered as medical devices under Directive 93/42/EEC or as in vitro diagnostic medical devices under Directive 98/79/EC it is crucial to differentiate in legal terms between medical device applications and lifestyle/well-being applications.

  An mHealth application becomes a medical device when its purpose is to initiate or regulate medical therapy, when it provides a medical diagnosis or constitutes a screening process or a prevention measure. Screening or prevention health apps could for example be smartphone apps that assess the degeneration risk on the basis of photos for example of skin lesions.

  In this context, there is need for action. It needs to be specified that these types of apps are subject to the medical devices Directive 93/42/EEC. As such, ESIP strongly advocates the establishment of a process of independent authorisation by the designated body of the application's performance to ensure the efficacy, functionality and proof of

positive risk benefit ratio. In addition, full transparency regarding the benefits and risks of the app is necessary. A simple self-declaration by manufacturers – e.g. for medical devices of risk category I - is not sufficient for mHealth apps which offer therapy, diagnosis, screening or prevention as defined above.

3.4. Patient safety and transparency of information

- What good practices exist to better inform end-users about the quality and safety of mHealth solutions (e.g. certification schemes)? Which policy action should be taken, if any, to ensure/verify the efficacy of mHealth solutions? How to ensure the safe use of mHealth solutions for citizens assessing their health and wellbeing)

  It is necessary to ensure that all persons involved in the process of gathering data through mHealth and digital media solutions are fully aware of their role and a secure information pathway is established. A necessary prerequisite for this is the education of patients for an appropriate use of m-health tools.

  In addition, the information on health contained in mHealth solutions should be independent. The issuer has to be clearly identified by the user. ESIP suggests a "certification system" for new mHealth solutions in order to guarantee the quality and independency of the information.

3.5. mHealth role in healthcare systems and equal access

- Do you have evidence on the uptake of mHealth solutions within EU's healthcare systems? What good practices exist in the organisation of healthcare to maximise the use of mHealth for higher quality care (e.g. clinical guidelines for use of mHealth)? Do you have evidence of the contribution that mHealth could make to constrain or curb healthcare costs in the EU? What policy action could be appropriate at EU, as well as at national, level to support equal access and accessibility to healthcare via mHealth?

  A systematic analysis of studies on mHealth (or eHealth) solutions is not available.

  Nevertheless, a number of studies have been carried out in the field of telemedicine, for example telemonitoring of patients. Similar advantages might be expected from the use of mHealth solutions as for telemonitoring of patients, for example: provision of care to chronically ill patients in structurally weak regions, reductions in in-patient treatments and associated cost savings. However, large, randomised, controlled trials comparing the treatment of heart failure patients with and without telemonitoring, have shown no significant differences in mortality rates and incidences of hospitalisation (Telemonitoring in patients with heart failure, Chaudhry SI. et al. 2010; 363 (24), 2301–2309; Impact of Remote Telemedical Management on Mortality and Hospitalizations in Ambulatory Patients with Chronic Heart Failure, Koehler F et al. Circulation 2011; 123(17):1873-1880).

  Therefore, stronger evidence-based studies on the usefulness of mHealth solutions are required. These studies should aim to demonstrate the cost-effectiveness and added value of mHealth solutions in comparison with the standard clinical care.

3.6. Interoperability

- What, if anything, do you think should be done, in addition to the proposed actions of the eHealth Action Plan 2012-2020, in order to increase interoperability of mHealth

solutions? Do you think there is a need to work on ensuring interoperability of mHealth applications with Electronic Health Records? And if yes by whom and how?

The proposed integration of mHealth apps into the national public health systems will depend on the current level of development of national rules in the Member States governing eHealth and mHealth. It is necessary to ensure data minimizing and the protection of personal data before considering increasing the interoperability of mHealth solutions. Security should not be jeopardised just to improve interoperability.

Nevertheless, there could be a need for ensuring that mHealth applications are interoperable not only with the Electronic Health Records (EHR) but also with other healthcare solutions. mHealth applications could provide valuable information about the patient which could be captured by a centralised EHR system. It would be the role of the owner/operator of the EHR system, under national rules, to enable the exchange data between healthcare supporting applications (e.g. through the use of web services).

3.7. Reimbursement models

- Which mHealth services are reimbursed in the EU Member States you operate in and to what extent? What good practice do you know of that supports refund of mHealth services?

  In order to obtain reimbursement by the SHI funds mHealth services need to be able to demonstrate patient-relevant benefit in comparative and prospective studies, ideally demonstrating at least equivalent effectiveness compared to the standard clinical care as well as proof of a positive risk benefit ratio and efficacy

  Examples for mHealth offered by SHI funds:

  Statutory health insurance funds and their umbrella organisations offer apps for free download to insured persons with information and counselling on various health topics as well as mHealth solutions providing monitoring services. Available free apps cover topics such as: early diagnosis check-ups; dental prophylaxis; vaccination; prenatal care; check-ups for children; lists of physicians and medical specialists, hospitals and clinics in the surrounding area; accident and first aid tips and information about complementary benefits.

  Finally, it should be noted that most business models in mHealth are still in the development stage; their success will depend on the (local) situation in the Member States.

3.8. Liability

- What recommendations should be made to mHealth manufacturers and healthcare professionals to help them mitigate the risks posed by the use and prescription of mHealth solutions?

  Key to mitigating the risks posed by the use and prescription of the mHealth solutions is the establishment of a reliable system of advanced authorisation and of reliable authentication mechanisms. Using mechanisms such as Public Key Infrastructure (PKI), the authenticity of the healthcare professional can be assured, increasing security through non-repudiation, which can later be used should legal questions arise. mHealth manufacturers need to collaborate with healthcare professionals, health insurance funds and health authorities when considering the potential risks involved if/when an solution is

adopted by the healthcare professional community. Existing risk management's procedures in the healthcare sector should be extended to the mHealth sector.

3.9. Research and innovation in mHealth

- Could you provide specific topics for EU level research & innovation and deployment priorities for mHealth? How do you think satellite applications based on EU navigation systems (EGNOS and Galileo) can help the deployment of innovative mHealth solutions?

  ESIP proposes the following topics for EU level research & innovation in mHealth:

  - mHealth aimed at providing better quality of care
  - mHealth aimed at better patient compliance
  - mHealth tools for exchange of clinical guidelines between health professionals
  - mHealth tools for health promotion and prevention

  As regards implementation of mHealth solutions, priorities for research and innovation should include:

  - Data protection and data security (personal data protection and functioning of the solutions)
  - Clear delimitation between medical device applications and lifestyle/well-being applications.
  - Liability (manufacturer, competent authorities, health professionals, SHI funds)

3.10. International cooperation

- Which issues should be tackled (as a priority) in the context of international cooperation to increase mHealth deployment and how? Which good practice in other major markets (e.g. US and Asia) could be implemented in the EU to boost mHealth deployment?

  International cooperation should be sought in the development of voluntary and non-binding international standards in mHealth, for example through existing international mechanisms and organisations such as ISO - International Organisation for Standardisation.

3.11. Access of web entrepreneurs to the mHealth market

- Is it a problem for web entrepreneurs to access the mHealth market? If yes, what challenges do they face? How can these be tackled and by whom? If needed, how could the Commission stimulate industry and entrepreneurs involvement in mHealth, e.g. through initiatives such as "Startup Europe" or the European Innovation Partnership on Active and Healthy Ageing?

  Entrepreneurs need to ensure that their mHealth solutions comply with the commonly established rules governing for example, data protection, authorisation mechanisms and interoperability with other applications.

  .