Position Paper on mHealth

Brussels, 29 September 2015

EXECUTIVE SUMMARY

The continued growth of mobile health (mHealth) solutions has the potential to provide countless opportunities for EU citizens, public health services and businesses. DIGITALEUROPE as the voice of Europe's digital technology industry calls on policy-makers to put in place the right framework conditions that will enable these solutions to thrive in the EU, in order toincrease the competitiveness of Europe in an area that is strongly developing globally as well as to solve the pressing challenges faced by European healthcare systems. While the risks associated with the use of mHealth applications should be clearly addressed, the focus of EU policy makers should be on fostering its opportunities. The European Commission took an important first step in April 2014 through the launch of its public consultation on mHealth to help identify the right way forward to unlock the potential of mHealth in the EU. As the European Commission continues to consider options for future action, DIGITALEUROPE believes any future activities within the field of mHealth should focus on the following measures:

- **Adequacy of Current EU Legal Framework** – Resist the temptation to introduce a dedicated legal framework for mHealth in the form of a Directive or Regulation as the existing EU regulatory framework for the safety and performance of medical devices has supplied a sound foundation against which technological innovations can be assessed;

- **Protection of Personal Data** – Harmonise privacy rules in the field of healthcare across Member States and follow a risk-based approach in order to both ensure privacy and embrace on-going data innovation; Promote a soft law approach by encouraging codes of conduct and guidelines.

- **Opportunities of Big Data** – Adapt the current regulatory framework to the borderless nature of big data while encouraging the use of de-identified, aggregate and properly secured health data;

- **Safety of Applications** – Emphasise that only those solutions that meet the definition of a medical device should face additional scrutiny as their potential malfunction could lead to adverse risk on user's health;

- **Impact on Healthcare Systems** – Encourage the European Commission's to continue its efforts to stimulate the adoption of mHealth technologies in the Member States through Horizon 2020 to create scalable products;

- **Encouraging Interoperability** – Promote the need for industry-led standards and certifications to increase the interoperability of Electronic Health Records (EHRs) information collected via mHealth services;

- **International Cooperation** – Encourage the European Commission to address any future additional mobile device certification requirements at the international level through the use of guidelines to ensure regulatory predictability for economic operators;

- **Market Access** – Promote the use of EU funds coupled with increased confidence in venture capital funding to address some of the weaknesses that hinder the entry of innovative mHealth solution to the EU market.

DIGITALEUROPE
Rue de la Science, 14 - 1040 Brussels [Belgium]
T. +32 (0) 2 609 53 10 F. +32 (0) 2 431 04 89
www.digitaleurope.org | info@digitaleurope.org | @DIGITALEUROPE
Transparency register member for the Commission: 64270747023-20

1. Introduction

Today, EU healthcare systems are facing significant challenges that are creating concerns about the sustainability of healthcare delivery in the future. The combination of an increased prevalence of chronic diseases and a growing ageing population are exacerbating the burden on costs associated with healthcare delivery across multiple EU Member States.

While there are many problems in EU Member State healthcare systems which need to be addressed, the use of mobile and wireless technologies has the potential to transform the face of health service delivery across the EU and reduce some of the costs threatening the system. mHealth has the ability to act as a valuable additional tool in the provision of care while supporting patients' empowerment and motivation, facilitation contacts between physicians and patients living in remote areas, and improving the quality of health service delivery. If deployed effectively, mHealth solutions will allow patients to be connected to services which include health information on demand while allowing for the 'real time' monitoring of chronic conditions such as diabetes and asthma.

We therefore welcome that the European Commission has recognised the important role that mHealth solutions can play in improving the lives of citizen's and reducing public healthcare costs as noted in its April 2014 Green Paper.[1] DIGITALEUROPE supports the objective to develop an action plan to seize the opportunities of mHealth and enable EU based mHealth application developers to compete globally.

With this paper, DIGITALEUROPE would like to make an initial contribution to the debate surrounding the future of mHealth solutions in Europe. We would like to stress that mHealth is no different from other areas of eHealth in its needs to adopt accepted standards and interoperable technologies. We believe that the use of industry-led standardised solutions would enhance efficiency, reduce cost and accelerate market entry. Further, this paper sets out a number of policy recommendations with a view to facilitating the expansion of mHealth technologies across the EU.

2. Adequacy of the Current EU Framework

As the European marketplace for mobile applications continues to develop, it will be of critical importance for economic operators to face an environment of regulatory predictability and certainty. When it comes to the field of medical devices, the existing EU regulatory framework has provided this necessary certainty by supplying a sound foundation for which technological innovations can be assessed. The 2007 revision of the framework explicitly brought software – including applications – into the regulatory scope and sufficiently clear definitions and guidance (i.e. MEDDEV on stand-alone software) exists to determine whether a given application is intended to be used specifically for diagnostic and/or therapeutic purposes.

The new Medical Devices Regulation (and the ensuing guidance) should build upon the merits of the existing regulatory approach, which enables both a high level of safety and cost-efficient market access for innovative products to the benefit of patients and healthcare professionals. We are concerned with the aim of the European Parliament to bring products with unspecified 'indirect' medical purposes into the scope of the Regulation. This will unjustifiably qualify a number of non-invasive and non-medical products such as wellbeing and lifestyle applications as well as general-purpose consumer electronics such as smartphones and tablets as medical devices.

We agree that, if harmonised by the Medical Device Regulation, the current regulatory structure can adequately govern mHealth. Further, medical device status and classification ought to be the rule against which all medical

---

[1] COM(2014) 219 final

DIGITALEUROPE
Rue de la Science, 14 - 1040 Brussels [Belgium]
T. +32 (0) 2 609 53 10 F. +32 (0) 2 431 04 89
www.digitaleurope.org | info@digitaleurope.org | @DIGITALEUROPE
Transparency register member for the Commission: 64270747023-20

2

tools are measured for safety, including mHealth apps. However, we feel ambiguities in the current guidance must be clarified and a clear policy statement made that regulators shall not enforce the Medical Device Directive against consumer-facing mHealth apps unless the apps: (a) are designed to be used to be used, directly or indirectly, by medical experts (i.e. not consumer-facing in reality); (b) could be perceived by users as providing medical guidance (as a substitute for a professional); or (c) present a clear risk to user health.

Where the "medical device" status is unclear, companies and regulators should cooperate to find a reasonable balance between risk prevention and service provision.

Furthermore, the Commission should encourage worldwide harmonisation based on these laws.

When it specifically comes to the field of mHealth, we caution against the introduction of a dedicated legal framework in the form of a Directive or Regulation. Such an approach could fragment the legal environment and foster regulatory uncertainty in the face of future innovation. We believe that the EU institutions should instead put in place a flexible system (similar to the approach taken by the US Food and Drugs Administration in its Guidelines on Mobile Medical Applications) which would aim to be future proof and evolve in parallel with technological advancements so as to ensure regulatory certainty all over the EU.

3. Protection of Personal Data

Although concerns are often raised about the processing of health data in the mHealth context, the current EU data protection framework as spelled out in the 95/46/EC Directive provides a comprehensive and coherent set of rules that protect citizens' personal data across all technology platforms, including mobile devices, with specific provisions for special categories of data such as health data. This framework has resulted in stringent Member States legislation regarding the processing of health data, which forbids any unwanted sharing with third parties (with derogations allowed only for reasons of public interest). These provisions are complemented by the ePrivacy Directive, which prescribes that consent and clear and comprehensive information to the user are necessary in order to place data on, and retrieve it from, devices. Furthermore, the revision of Europe's current rules as seen in the draft General Data Protection Regulation aims to create more harmonised conditions across the EU.

Given that the aforementioned rules apply in the mHealth context, we believe there is no need for technology-specific security requirements that would apply to the processing of health data involving mobile platforms. We instead encourage Member States to follow a risk-based approach in order to both ensure privacy and embrace data innovation in the future. It will be fundamental for risk to be set as the general criterion in determining how the fundamental right to the protection of personal data may be safeguarded while ensuring that personal data is adequately protected without imposing inappropriate or disproportionate burdens. In addition, institutions, both at European and national level, should adopt a soft law approach by promoting codes of conducts and guidelines addressing specific aspects of privacy related to mHealth. The current initiative taken by the European Commission for an industry-led code of conduct on privacy for mHealth applications follows this approach.

We strongly support EU-wide harmonization. Likewise, we believe that the current data protection rules, in principle, meet the needs of mHealth, subject to some clarifications:

- Health data sits along a sensitivity scale from "trivial" to "medical"

- Security expectations relating to health data should follow the scale from "no more than standard practice for name, email and address" to "full ISO27000 or equivalent" depending on the significance/sensitivity of the data.

- Authorities primary role is assist companies in determining adequacy of security; enforcement reserved for clear cases of negligence, misconduct, or bad faith by company.

DIGITALEUROPE
Rue de la Science, 14 - 1040 Brussels [Belgium]
T. +32 (0) 2 609 53 10 F. +32 (0) 2 431 04 89
www.digitaleurope.org | info@digitaleurope.org | @DIGITALEUROPE
Transparency register member for the Commission: 64270747023-20

3

When it comes to mHealth application developers and users, we firmly believe that no specific technology or operational mandates should be introduced and that the guiding principles of 'data minimisation', 'data protection by design' and 'data protection by default' are best upheld by leaving room for a variety of implementations based upon an mHealth applications functionality and the different levels of risk involved. Privacy by design should be considered a process for ensuring that data protection is carefully considered in the design and implementation of products, but should by no means be a technology-specific requirement to be embedded with products as this would go against the concept of technological neutrality. Furthermore, imposing design mandates in the field of mHealth would directly challenge the technology neutrality of the legal framework, would result in significant burdens and would hinder rather than promote user privacy and security by creating a single point of failure.

Application developers should instead be encouraged to focus on the actual outcomes in terms of privacy and security, rather than having to comply with the technology-specific or mHealth specific requirements from the start of application development.

4. Opportunities of Big Data

The ability for mHealth solutions to take advantage of 'Big Data' can only be realised if Europe's regulatory framework is adopted to the borderless nature of 'Big Data' and allows for the optimal flows and usage of data. The development of 'Big Data' in the context of mHealth requires a regulatory framework that allows for the use of de-identified, aggregate and properly secured health data that can deliver innovations for the benefit of patients and society. It should promote similar measures to those encouraged to unleash the potential of other economic and social sectors including: the promotion of open data flows, the facilitation of access to the best technologies on a global scale, the encouragement of the uptake of cloud computing, the improvement of science and education systems in the field of data analytics, etc.

It is worth stressing that while the current EU data protection framework lays down safeguards to the protection of citizens' health data it is at the same time the single most significant obstacle to capturing value from 'Big Data' in that it limits the possibility of data sharing across organisations and borders (in some cases, through local data server requirements) and strictly limits processing to the specific purposes for which the data was initially collected. While these measures aim to protect citizens' privacy, they make secondary use of data for healthcare and research complicated if not impossible. Regrettably, the draft General Data Protection Regulation would create even more obstacles to the use of data-driven technologies.

More specifically, within the field of healthcare DIGITALEUROPE strongly encourages the continued deployment of Electronic Health Records (EHRs) across EU Member States. Without EHRs, Europe's healthcare systems lack a major foundation to generate 'Big Data' by pooling single patients' health data in standardised formats in order to support more personalised care.

We agree that facilitating secure and responsible exchange of big data will benefit everyone involved. Beyond the requirements stated (de-identified, aggregate, and properly secured), health (big) data must indicate the reliability of the source so experts can weigh this into their results.

5. Safety of Applications

When it comes to evaluating and setting the safety standards of mHealth applications, it is important to keep in mind the distinction between those mHealth solutions that meet the definition of a medical device and those that do not. We wish to note that the policy objective of any future EU regulatory framework applicable to

DIGITALEUROPE
Rue de la Science, 14 - 1040 Brussels [Belgium]
T. +32 (0) 2 609 53 10 F. +32 (0) 2 431 04 89
www.digitaleurope.org | info@digitaleurope.org | @DIGITALEUROPE
Transparency register member for the Commission: 64270747023-20

4

mHealth is to set out general safety and performance requirements for only those products that qualify as medical devices, as these pose potentially relevant health risks to citizens in the event of malfunction. Only a fraction of mHealth apps on the market today have a genuine medical purpose, while the vast majority are applications that provide lifestyle and wellbeing advice. In light of this, most mHealth applications available on the market today do not meet the definition of a medical device and should consequently not be subject to EU action to set high standards of safety and quality.

For those mHealth applications which are classified as medical devices, we believe the current certification & information display requirements applicable in the EU have proved effective. The 'intended purpose' principle along with the classification scheme, as provided for by the Medical Devices Directive, has proved to be up to the expectations of practitioners and users so far. Any further certification mechanisms or quality labels should be industry-driven and remain voluntary and affordable. Moreover, we support the continuous dialogue between patients, healthcare professionals, manufacturers and developers to ensure that these solutions are used safely and can effectively improve healthcare delivery.

6. Impact on Healthcare Systems

Much has been said about the lack of large-scale evidence proving the positive impact that mHealth solutions have had on cutting healthcare costs across Member States. Despite these claims, we firmly believe that there is consistent evidence that mHealth solutions can have a positive impact on healthcare delivery processes. Evidence has shown that mHealth solutions have led to fewer emergency admissions, hospitalisations and bed days per intervention as well as reduce mortality. We encourage public authorities to continue to study the impact of mHealth on reducing healthcare expenditure to counter negative sentiment surround mHealth and its potential to reduce healthcare costs.

Furthermore, despite its potential benefit to Europe's healthcare systems, mHealth uptake still remains limited in Europe. This stems from a lack of simple business models supporting the massive adoption of mHealth services and applications. Solutions deployed to date have been tailored and developed for specific regional or local authorities, each having different requirements, for specific use cases and situations. This has led to the current state of numerous pilots, but no mass-market adoption of mHealth due to the lack of interoperability and economies of scale.

We openly welcome the European Commission's attempts to address this problem through their efforts to stimulate the adoption of mHealth technologies in Member States. We believe that the new Horizon 2020 programme goes in the right direction in trying to learn from past experiences and design projects that can go beyond the current patchwork of pilots that have failed to create interoperable and scalable products. We encourage the European Commission to make sure that European funds, including cohesion policy funds, can be used to create large-scale access to innovative mHealth technologies for Europeans healthcare systems.

7. Encouraging Interoperability

DIGITALEUROPE believes that the actions contained in the eHealth Action Plan to foster the adoption of EU-wide standards remain valid to increase the adoption of interoperable mHealth products and services. Moreover, in light of the fast cycle of replacement in mHealth solutions compared with traditional medical devices, we believe the EU should promote industry-led standards and certifications in an effort to reduce burdens associated with certification and improving time to market for products.

DIGITALEUROPE
Rue de la Science, 14 - 1040 Brussels [Belgium]
T. +32 (0) 2 609 53 10 F. +32 (0) 2 431 04 89
www.digitaleurope.org | info@digitaleurope.org | @DIGITALEUROPE
Transparency register member for the Commission: 64270747023-20

5

Furthermore, we believe that the interoperability of EHRs with information collected via mHealth services is essential to improve the quality, safety and efficiency of care while seeking to improve citizens' inclusion and engagement. A 'holistic' approach to interoperability will enable healthcare systems to easily share EHRs across providers and citizens while benefiting from the interconnected value of health IT apps and wearable technologies.

8. International Cooperation

DIGITALEUROPE warns against the risk that mobile devices may fall victim to over-regulation by additional certification requirements on top of those traditionally foreseen for their usual product category. Moreover, such over-regulation could be combined with diverging regional regulatory approaches across the globe leading to high costs for venders as they will need to set up dedicated certificatory compliance structures for each region.

We therefore call for a certain level of international convergence and believe that this would be best addressed at the international level by setting up guidelines or even an agreement (e.g. in the context of the IMDRF), to ensure regulatory predictability for economic operators.

Moreover, we wish to note that the current negotiations for a Trade in Services Agreement (TiSA) represents an opportunity to ensure cross-border availability of mHealth services.. The inclusion of mHealth services could provide companies with the international legal framework to reach economies of scale.

9. Market Access

As previously mentioned, DIGITALEUROPE believes that the use of EU funds are an important tool to address some of the weaknesses that hinder the entry of innovative mHealth entrepreneurs to the European healthcare market. We believe that Horizon 2020 has the potential to address this problem as long as the pilot projects keep in mind the goal to reach economies of scale.

We also wish to note that corporate venture capital must also play a role in increasing market access for mHealth solutions. It is essential for European policies to create the confidence for the venture-funding market to invest in innovative, but often high-risk mHealth applications and generate the necessary returns on investment.

We also wish to note that along with funding and regulatory challenges, the lack of existing interoperable standards remains a major barrier to market entry. This is arguably the most serious obstacle for small mHealth entrepreneurs to enter the healthcare market and grow their business. The EU-wide adoption of already available global standards and specifications will be key in creating better market entry conditions in this respect.

10. Conclusion

mHealth has the potential to be a transformative force changing when, where and how healthcare is provided to EU citizens. This growing technological trend has the ability to cut the cost of providing healthcare, improve the quality of care and reach patients in remote locations. As such, European policy makers must work to create an environment that will allows European based mHealth application developers to thrive so that these new solutions can have the highest possible impact on our society and economy. The European Commission has recognised this need and has taken an important first step in through its Green Paper while seeking the opinion of stakeholders through the corresponding public consultation. In this paper, we have out the European ICT industry's perspective of what are the most important measures for the EU to take when it comes to mHealth public policy.

DIGITALEUROPE
Rue de la Science, 14 - 1040 Brussels [Belgium]
T. +32 (0) 2 609 53 10 F. +32 (0) 2 431 04 89
www.digitaleurope.org | info@digitaleurope.org | @DIGITALEUROPE
Transparency register member for the Commission: 64270747023-20

6

For more information please contact:
Jean-Marc Leclerc, DIGITALEUROPE's Policy Director
+32 2 609 53 25 or jeanmarc.leclerc@digitaleurope.org

ABOUT DIGITALEUROPE

DIGITALEUROPE represents the digital technology industry in Europe. Our members include some of the world's largest IT, telecoms and consumer electronics companies and national associations from every part of Europe. DIGITALEUROPE wants European businesses and citizens to benefit fully from digital technologies and for Europe to grow, attract and sustain the world's best digital technology companies.

DIGITALEUROPE ensures industry participation in the development and implementation of EU policies. DIGITALEUROPE's members include 59 corporate members and 35 national trade associations from across Europe. Our website provides further information on our recent news and activities: http://www.digitaleurope.org

DIGITALEUROPE MEMBERSHIP

Corporate Members

Acer, Alcatel-Lucent, AMD, Apple, BlackBerry, Bose, Brother, CA Technologies, Canon, Cassidian, Cisco, Dell, Epson, Ericsson, Fujitsu, Google, Hitachi, Hewlett Packard, Huawei, IBM, Ingram Micro, Intel, iQor, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, Loewe, Microsoft, Mitsubishi Electric Europe, Motorola Mobility, Motorola Solutions, NEC, Nokia, Nvidia Ltd., Océ, Oki, Oracle, Panasonic Europe, Philips, Pioneer, Qualcomm, Ricoh Europe PLC, Samsung, SAP, SAS, Schneider Electric IT Corporation, Sharp Electronics, Siemens, Sony, Swatch Group, Technicolor, Texas Instruments, Toshiba, TP Vision, Western Digital, Xerox, ZTE Corporation.

National Trade Associations

Belarus: INFOPARK
Belgium: AGORIA
Bulgaria: BAIT
Cyprus: CITEA
Denmark: DI ITEK, IT-BRANCHEN
Estonia: ITL
Finland: FTTI
France: Force Numérique, SIMAVELEC
Germany: BITKOM, ZVEI

Greece: SEPE
Hungary: IVSZ
Ireland: ICT IRELAND
Italy: ANITEC
Lithuania: INFOBALT
Netherlands: Nederland ICT, FIAR
Poland: KIGEIT, PIIT
Portugal: AGEFE
Romania: ANIS, APDETIC
Slovakia: ITAS

Slovenia: GZS
Spain: AMETIC
Sweden: Foreningen Teknikföretagen, IT&Telekomföretagen
Switzerland: SWICO
Turkey: ECID, TESID, TÜBISAD
Ukraine: IT UKRAINE
United Kingdom: techUK

DIGITALEUROPE
Rue de la Science, 14 - 1040 Brussels [Belgium]
T. +32 (0) 2 609 53 10 F. +32 (0) 2 431 04 89
www.digitaleurope.org | info@digitaleurope.org | @DIGITALEUROPE
Transparency register member for the Commission: 64270747023-20

7