

The Consumer Voice in Europe

HEALTH IN THE TIME OF SMART PHONES

BEUC position paper on mobile health



Contact: Ilaria Passarani - Francesca Cattarin – health@beuc.eu

BUREAU EUROPÉEN DES UNIONS DE CONSOMMATEURS AISBL | DER EUROPÄISCHE VERBRAUCHERVERBAND
Rue d'Arlon 80, B-1040 Brussels • Tel. +32 (0)2 743 15 90 • www.twitter.com/beuc • consumers@beuc.eu • www.beuc.eu
EC register for interest representatives: identification number 9505781573-45



Co-funded by the European Union

Ref: BEUC-X-2016-112 - 07/11/2016

Why it matters to consumers

How many steps did you walk today? What should you have for a healthy dinner? What's your sleeping pattern? Because smartphone applications and connected medical devices can answer those questions in just a few clicks, mobile health (mhealth) is gaining ground among EU consumers.

However, most health applications available do not have a privacy policy. When they do, apps fail to protect consumers' personal data. Beside those privacy concerns, consumers can hardly assess how useful and reliable those tools are. This ultimately questions the benefits on public health.

Summary

Mobile health (mhealth) is an emerging field that has the potential to transform healthcare. Mobile devices and related software ('applications' or 'apps') may bring immediate answers to consumers, empower them and potentially unburden the healthcare systems.

Mhealth solutions include medical devices that deliver information on specific chronic conditions but also lifestyle and wellbeing apps. The already enormous profits that derive from this successful market are expected to skyrocket in the next years.

However, mhealth entails potentially serious risks for consumers. To reverse the trend, policy makers should take the following measures at the European Union (EU) level:

1. Clearly define 'mhealth'

A more effective regulatory framework should cover *all* mhealth solutions. This would oblige manufacturers to play by the same rules and provide the same high quality level of information to consumers. At the moment, only a minority of tools is covered by specific laws, i.e. those regulating medical devices and in vitro diagnostic devices.

2. Ensure legal accountability and right to redress

Bad quality mhealth solutions may harm consumers. But who is responsible? Liability should be clear for all mhealth solutions, not just for medical devices and in vitro diagnostic. Consumers should also be given tools to claim redress.

3. Guarantee privacy and data protection

Consumers have the right to data protection, especially when related to their health. Privacy settings should be embedded from the manufacturing stage. As for data collection, it should be limited to the essential functioning of the device.

4. Set simple and fair Terms and Conditions

Consumers can effectively understand and take decisions only if terms and conditions are clear and transparent.

5. Ensure security at all stages

Mhealth solutions should embed specific safeguards at each stage of data processing. This should include the encryption of patients' data and authentication mechanisms to beef up protection.

6. Label apps' target audience

Some apps are intended for consumers while others aim to support healthcare professionals. To prevent consumer misuse, developers should specify the target audience of each app.

7. Ensure mHealth does not widen gaps in access to care

The uptake of mhealth goes hand in hand with mobile internet availability, which is unequal from one country to another. To prevent health disparities within the EU, Member States need to promote digital and health literacy before promoting mhealth.

Scope of the paper

Mhealth is a broad concept which comprises a wide range of different solutions. For example, when mhealth is about a wearable and connected device, it is considered as a normal consumer good that might be classified under the novel notion of Internet of Things (IoT). Conversely, other mhealth solutions can be defined as a medical device.

The different components that make up the whole mhealth "ecosystem" are not fully considered in the text. The aim of this position paper is to highlight the most consumer-relevant issues at stake in mobile health and to suggest ways to boost consumer protection.

Contents

1. Safety first: consumers deserve high quality mobile health.....	5
2. Legal protection: liability and consumers' right to redress	7
3. Health data deserves the strongest privacy protection.....	7
3.1. Privacy by design	7
3.2. Health should get special treatment	8
3.3. Big data and risk of discrimination	9
4. Terms and conditions: from complex to simple.....	10
5. Security matters	11
6. Different apps, different users.....	12
7. There is no mobile health without internet access & digital literacy	12
7.1. Consumers engagement in the development of mhealth tools.....	13

Introduction

Mobile health (hereafter 'mHealth') can be defined in several ways. One of the most complete explanations is "using mobile and wireless devices to improve health outcomes, healthcare services and health research"¹. Mhealth thus brings medical and public health practices closer to consumers through mobile devices such as wearable watches, bracelets and mobile phones, using software called applications - or apps for short.

The sustainability of European healthcare systems is at stake for various reasons including the ageing population, skyrocketing prices of medicines², the prevalence of chronic diseases and citizens' increased expectations for high quality health services. In such a context, the large scale deployment of mhealth tools could help address some of these challenges. Moreover mhealth can contribute to improve the quality of care while empowering consumers.

Mobile health can be used for simple but important tasks such as sending SMSs to remind the patient when and how to take a medicine or keep medical appointments. More specifically, mhealth tools for self-monitoring can empower consumers by making them more responsible and aware of their conditions.

Remote solutions can also ease the burden of healthcare systems by performing part of their services. Real-time remote monitoring can be particularly useful in the management of chronic diseases, especially when hospitals and nursing homes have limited capacity³. These solutions can benefit not only consumers who are unable to move by reaching them into their homes, but also travelling individuals who can access self-generated information and transmit it to their health professionals.

Another potential benefit for consumers is the introduction of the Electronic Health Records (EHR)⁴. Such files include information on patient age, treatment progress, medications, medical history, laboratory data, to name a few. Thanks to mobile health, users can transfer the health data generated on their mobile devices to their personal health records or healthcare providers. This represents an easy extra source of information to help the healthcare professional when treating a patient.

Mhealth is thus rapidly emerging as a complementary way of delivering healthcare, facilitated by the proliferation of smartphones, tablets and the 3G and 4G networks. According to a recent report, currently around 165,000 mhealth apps are available to consumers, a number that has soared in the past two years⁵. The forecasts for this market are enormous with some estimates expecting to reach the equivalent of 23 billion dollars in 2017⁶, to reach 103.23 billion by 2022⁷.

¹ See <http://www.himss.org/definitions-mhealth>

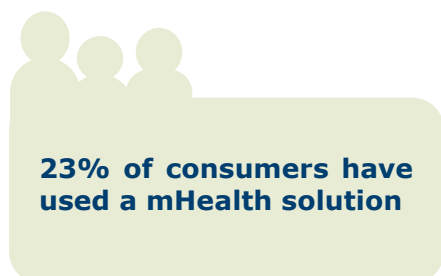
² http://www.beuc.eu/publications/beuc-x-2015-104_access_to_medicines.pdf

³ <https://www.telenor.com/wp-content/uploads/2012/05/BCG-Telenor-Mobile-Health-Report-May-20121.pdf>

⁴ <http://www.beuc.eu/publications/2011-00399-01-e.pdf>

⁵ <http://www.imshealth.com/files/web/IMSH%20Institute/Reports/Patient%20Adoption%20of%20mHealth/mHealth-Apps-by-Category-2015.pdf>

⁶ GSMA and PwC, Touching lives through mobile health - Assessment of the global market opportunity February 2012.



Yet, many Europeans do not associate their mobile devices with health: only 23% of consumers have used a mHealth solution⁸ whilst 77% of consumers have never used their phone for health-related activities⁹. Despite its huge potential, mHealth raises important questions about how consumers' personal data is collected, generated and analysed. Such concerns should be addressed before mobile health is rolled out on a larger scale.

In the absence of convincing data demonstrating the advantages of mhealth¹⁰, and until rigorous evidence becomes available, the EU should put in place more safeguards for consumers' health and rights.

1. Safety first: consumers deserve high quality information when accessing mobile health

Some mhealth solutions fall into the scope of medical devices, which have been clarified in the Medical Devices and In vitro diagnostic medical devices regulations (hereafter the Regulations)¹¹. Thanks to the new Regulations¹², mhealth apps with a *medical purpose* will be classified as medical device and hence will be subject to stricter safety requirements¹³.

⁷ <http://www.medgadget.com/2016/02/global-m-health-applications-market-worth-103-23-billion-usd-by-2022.html>

⁸ Boehm. E, Mobile healthcare's slow adoption curve, 2011. Forrester Research Inc. Reported in the European Commission's Green Paper on mHealth

⁹ Boehm. E, Mobile healthcare's slow adoption curve, 2011. Forrester Research Inc. Reported in the European Commission's Green Paper on mHealth

¹⁰ M. Tomlinson et al. (2013), 'Scaling up mHealth: Where is the evidence?', PLoS Medicine, <http://www.plosmedicine.org/article/info%3Adoi%2F10.1371%2Fjournal.pmed.1001382>, 12 Feb 2013.

¹¹ http://www.beuc.eu/publications/beuc-x-2013-031_ipa_medical_devices-beuc_updated_position-final.pdf

¹² http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_10617_2016_REV_1&from=EN A deal was reached between the Council and the European Parliament; however the final version of the text will be available only after the plenary vote in the Parliament.

¹³ According to the definition provided in the Regulation, a mhealth app will be classified as "medical" if such app is specifically designed for a medical setting and for performing a medical task. This will include apps for the purpose of prevention, diagnosis and treatment diseases.

In practice this means that once a mobile health app is classified as a medical device it is subject to obligations similar to those currently applied for the monitoring of safety of medicines. In other words, manufacturers will have to report serious incidents on the European database on medical devices (Eudamed). The subsequent post-market surveillance will require app developers to report on safety annually. Consumers will have the chance to contact a legitimate and competent partner in case of problems caused by the use of the app (see point 2).

Overall, the new Regulations will strengthen the rules for developers while increasing consumers' safety when using mhealth solutions for a medical purpose. However, these are only a small minority in the whole market¹⁴.

All the other mhealth apps designed for *general purpose* will not be subject to the EU laws regulating medical devices. This means that lifestyle, fitness and well-being apps will only be subject to voluntary guidelines, which are expected to be published at the end of 2016¹⁵ and the General products safety legislation. Overall, this grey zone around the liability of software will cause great legal uncertainty¹⁶ and, in return, will weaken the legal protection for the many consumers who use mhealth to look for information and advice.

A recent report revealed that of more than 165,000 mhealth apps available worldwide, nearly two thirds focus on wellness issues like fitness, lifestyle & stress, and diet¹⁷. Given their big variety, it is not surprising that the security of tools and the accuracy of the information they provide are the main cause of concern for consumers and healthcare professionals towards mhealth¹⁸. Reports show that some devices fail to measure up, do not work as they should or lack clinical evidence¹⁹. In addition, some apps may be classified as 'informational' or 'entertainment' inadequate information. .

A high quality standard should define the manufacturing and marketing of all mhealth solutions. This would help to ensure the devices are reliable and provide correct and high-quality information, reduce the risk of getting measurement, diagnosis or treatment wrong. Such standards would finally clarify which rules have to apply to those mhealth devices which, as minor as they seem, can impact consumer's health.

A common international standard would be in line also with the resolution of the European Parliament on the eHealth Action Plan 2012-2020. It underlined the need for clear laws to ensure the development and safe adoption of ehealth-mhealth solutions²⁰.

¹⁴ mHealth Solutions Market by Connected Devices (Blood Pressure Monitor, Glucose Meter, Pulse Oximeter) Apps (Weight Loss, Women's Health, Personal Health Record, & Medication) Services (Remote Monitoring, Consultation, Prevention) - Global Forecast to 2020

¹⁵ http://www.ema.europa.eu/ema/index.jsp?curl=pages/news_and_events/events/2016/08/event_detail_001314.jsp&mid=WC0b01ac058004d5c3

¹⁶ <http://www.whitecase.com/publications/article/mobile-health-apps-are-they-regulated-medical-device>; <http://www.arnoldporter.com/en/perspectives/publications/2016/06/a-long-awaited-political-handshake-eu-medical>

¹⁷ <http://www.imedicalapps.com/2015/09/ims-health-apps-report/#>

¹⁸ <https://ec.europa.eu/digital-single-market/en/news/mhealth-green-paper-next-steps>

¹⁹ The New England Center for Investigative Reporting, Boston University, "Lacking regulation, many medical apps questionable at best", 18 November 2012

²⁰ Resolution of 14 January 2014, <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0010+0+DOC+XML+V0//EN>

Such a standard would also be a reliable indicator for healthcare professionals, patients and consumers organisations who would be able to promote certificated devices. These players should at the same time raise awareness about mhealth solutions and explain that these devices and apps can support healthcare but should in no case substitute for face-to-face contact.

2. Legal protection: liability and consumers' right to redress

As with all types of healthcare, flaws and errors in mHealth solutions may have major consequences for consumers' health. For example, a faulty heartbeat monitor may record an incorrect count, a healthcare professional could receive the wrong report or a patient could be given the wrong advice. Privacy breaches and wrongful data disclosure or sharing could also harm consumers, for example discriminating them in the workplace or in the insurance market.

So how can consumers be protected?

Liability for mHealth is a complex issue. The manufacturers and users can be diverse and sometimes intertwine with distributors and creators of mobile devices or related apps²¹. In addition, the range of options for healthcare providers to diagnose, advise, monitor and treat patients remotely can easily blur the line between a medical service and self-help. This grey zone can complicate medical professional liability, as a clear legislation applies only for medical devices.

Clearer and more comprehensive rules are therefore crucial to **safeguard consumers' right to redress for errors made by or resulting from mHealth manufacturing or production**. The scope of the manufacturer's liability should be clearly outlined in the model contract that users receive when they first download/open the app.

Specific rules should define the liability of all players involved in the life cycle of mhealth - or ecosystem - such as the device manufacturers, app developers, and data recipients. Consumers should have tools to seek redress and compensation (both individually and in collective actions) and dissuasive penalties should be introduced for abuses.

3. Health data deserves the strongest privacy protection


3.1. Privacy by design

The protection of personal information should be one of the core criteria to assess how reliable a mhealth solution is. Mobile health services and applications should be designed to be crystal clear about the processing of consumers' personal information. To do so,

²¹ FDA. (9 Feb 2015) Mobile Medical Applications -Guidance for Industry and Food and Drug Administration Staff <http://www.fda.gov/downloads/MedicalDevices/.../UCM263366.pdf> See the definitions of a mobile app manufacturer on pages 9-11.

such tools should have so called 'privacy by design', i.e. privacy and data protection features embedded in the device's core. Also, the default settings should set at the highest level of privacy protection possible. This is in line with the requirements of the General Data Protection Regulation (Article 25) and also with the recommendations of the European Data Protection Supervisor.²²

As stated in the EU data protection law, mhealth solutions owners should not collect more data than what is required to make the device function. In other words, companies should limit as much as possible their intrusion into individuals' privacy. Such attitude would help restoring consumers' trust. Almost half of consumers are indeed concerned about how their data is processed when they use mobile devices for health-related activities²³.



45% of consumers worry about how their data is processed when they use health-mobile devices.

Unfortunately this fear is confirmed by a recent study showing that 81% of applications available on the market had no privacy policy. When they did exist, privacy policies failed to protect data: 80% compiled personal data and 50% shared them with other parties²⁴.

Mhealth apps are no exception. In its "Appfail report"²⁵, the Norwegian Consumer Council found that a very popular fitness app, used by more than 45 million users, inadvertently collected personal data, tracking users when the app was not in use and sending the data to third parties²⁶.

In order to fully and effectively protect consumers' privacy, it is crucial that every stakeholder in the ecosystem applies the principle of Privacy by design and Privacy by default. Additionally, **consumers should have the possibility to revoke any prior consent given to a specific data processing, and to object to the processing of their data.** This has to be made possible without any technical or organizational constraint²⁷. Finally, the tools provided to register this refusal should be accessible, visible and efficient. Furthermore, since wearable connected devices are likely to replace existing items that provide usual functionalities, data controllers should offer an option to deactivate the device's connected feature and allow it to work as the original, unconnected item (e.g. there should be an option to disable the smart watches or glasses' connected functionality).

3.2. Health should get special treatment

Under the EU data protection law, health data is considered as a special category which merits additional protection and thus can only be processed under strict specific conditions. This special treatment covers the explicit consent of the user or when the

²² European Data Protection Supervisor. Opinion 1/2015 Mobile Health Reconciling technological innovation with data protection. 21 May 2015.

https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-05-21_Mhealth_EN.pdf

²³ Blue Chip Patient Recruitment. Leveraging Mobile Health Technology for Patient Recruitment, October 2012. Reported in the European Commission's Green Paper on mHealth

²⁴ <http://jama.jamanetwork.com/article.aspx?articleid=2499265>;

<http://bmcmmedicine.biomedcentral.com/articles/10.1186/s12916-015-0451-z>

²⁵ <http://fbrno.climg.no/wp-content/uploads/2016/03/Appfail-Report-2016.pdf>

²⁶ <http://www.forbrukerradet.no/side/runkeeper-tracks-users-when-the-app-is-not-in-use/>

²⁷ Applications GSM : vie privée en danger, Test Achats, Budget & Droit 234, mai-juin 2014

processing is necessary for a preventive or occupational medicine, or a health care service is carried out by a health professional.

As a means of example, personal data collected by tools that help patients monitor their blood pressure will certainly fall under the category of 'health data'. By contrast, the category of mhealth devices and applications such as those instructing users to perform routine fitness exercise, is less clear.

The soon-to-be rolled out General Data Protection Regulation (GDPR) introduces a broad definition of health data. However, information about fitness/lifestyle/well-being is not specifically mentioned, so although in most cases it would qualify as 'health data', this will not always be the case. Therefore the increased level of protection granted to health data might not be systematically applied. The Data Protection Authorities already attempted to clarify this question²⁸. Nevertheless, further legal guidance or clarification would be needed by regulators to avoid having to rely solely on a case by case analysis and on the discretionary judgement of the mHealth companies collecting and using the data.

Similarly, providers cannot simply consider the personal health/wellbeing data generated by mobile apps as user-generated content. This is particularly important given that the terms and conditions of use sometimes grant providers unfair extensive licenses to do almost anything they want with user-generated content, which are not covered by data protection rules.

3.3. Big data and risk of discrimination

The right of EU citizens to have their privacy and personal data protected is enshrined in the EU Treaty (Art 16.1 TFEU), in the EU Charter of Fundamental Rights (Art 7 and 8) and in the UN Declaration of Human Rights. It is also crystallised in the EU data protection legislation mentioned above.

But digital technology, big data and the proliferation of connected devices, such as fitness trackers that monitor and analyse every tiny aspect of our lives, greatly challenge our fundamental rights to privacy and data protection.

The privacy of consumers is constantly exposed. For example, some do not always realise that when they consent to download or use a health app, they authorise the app owner and/or third parties to collect and use unrelated information on their devices, such as their contacts and their internet search history.

Generally, mhealth can facilitate the information gathering and analysis of large amounts of health data (data mining), such as measurements and symptom descriptions. The data can be stored, combined and subsequently analysed in large databases, with the

²⁸ See EDPS Opinion 1/2015 https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-05-21_Mhealth_EN.pdf; see also Article 29 Working Party: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_annex_en.pdf

potential to boost healthcare and innovation. In jargon, experts in this field define this process as big data analysis²⁹ which can greatly benefit the whole society.

For example, big data has the potential to develop more advanced mechanisms for detection and prevention of diseases, draw new conclusions and therefore improve healthcare. However, since health data is particularly sensitive, the use of increasingly detailed data on a large scale raises very serious concerns. It is therefore essential to ensure that the collection, treatment, storage and disposal of health data are done under the highest standards of protection as required by the EU data protection law.

Mobile health services should not collect, store or share personal data without the informed and explicit consent of the consumer. Such consent must be sought again if there are any changes in the terms the consumer initially subscribed to. Users should be able to choose whether they consent to sharing their data anonymously to contribute to big data analyses. Also, consumers should always be able to access their data and to eliminate their digital information from mHealth tools. At the moment the industry does not fully comply with such requirements. Our Portuguese member DECO conducted an analysis on 17 storage cloud providers available on the market and noted numerous unfair terms detrimental to consumers³⁰.

In some cases, consumers may even be encouraged to provide their personal health data to app owners and/or related third parties. The German Federal Commissioner for Data Protection raised concerns about risks of disclosing personal data to third parties via health and fitness apps. Mr Voßhoff acknowledged that consumers may have short-term incentives to do it, such as disclosing them to private insurance companies in exchange for lower fees.

However, there may be unforeseen, long-term negative consequences for consumers³¹. As our Belgian member Test-Achats pointed out³², thanks to health profiling insurance companies will be in a position to unduly know a lot more about the health of their clients, allowing them to discriminate when setting their prices and reducing risk-taking to the minimum possible. Such profiling is easy to carry out through simple devices such as fitness bracelets, sleep cycle apps and calorie calculators. Unsurprisingly this practice is already in place, with insurance companies providing their clients with free self-measurement devices to track their health habits.

4. Terms and conditions: from complex to simple

Consumers can effectively control their privacy only if the terms and conditions that regulate this aspect are understandable to them. Therefore, when choosing a mhealth tool, **consumers should be able to access transparent and standardised**

²⁹ Green paper on mhealth

³⁰ <https://www.deco.proteste.pt/tecnologia/tablets-computadores/dicas/conteudos-na-cloud-como-proteger-por-morte-do-utilizador>

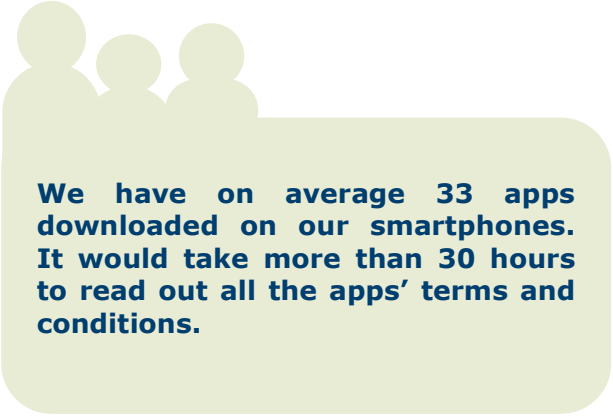
³¹ Press release. Andrea Voßhoff warnt vor dem Einsatz von Fitness-Apps durch Krankenkassen. July 2015.

http://www.bfdi.bund.de/DE/Infothek/Pressemitteilungen/2015/18_WarnungVorFitnessapps.html?nn=5217040

³² <https://www.test-achats.be/action/espace-presse/communiqués-de-presse/2015/privacy>

information. It must include the type of personal data that will be collected, when, for which purposes, whether it will be shared with third parties, if so who are those third parties, etc. Importantly, this information needs to be clear, easy to understand and concise.

At the moment it is very difficult for the average consumer to understand the terms and conditions of mobile apps. It is then no surprise most people accept the terms without knowing what the company behind gives itself the right to do. The Norwegian Consumer Council ran a campaign and filmed participants reading out in one go all the terms and conditions of 33 popular apps, the average number Norwegians have on their phones. It took them more than 30 hours³³.



We have on average 33 apps downloaded on our smartphones. It would take more than 30 hours to read out all the apps' terms and conditions.

Safety warnings about the use of data should appear in a clearer and more direct way, for example through the form of short and clear questions addressed to consumers prior to the download of the app. Through these direct questions, consumers would be asked whether they are aware that their data could be sold to third parties, for which purpose and to which extend. This would help end-users to make a more informed choice and better understand the consequences of some choices³⁴.

5. Security matters

Privacy is strictly linked with security. If a mobile health solution is not secure, unnecessary, unlawful and unauthorized processing of health data can occur, which means privacy cannot be guaranteed.

This is particularly likely for mobile solutions that can be easily misplaced and lost, becoming the prey of hackers. This can happen for example with healthcare professionals accessing health information from a mhealth device, or with patients storing their data on a personal health record application. Therefore, as the European Commission suggested in its Green paper³⁵, mhealth solutions should comprise specific and suitable safeguards such as encryption of patients' data and appropriate authentication mechanism.

In practical terms, mhealth solutions involving sensitive health information should always request users to go through an authentication mechanism in order to access and update their data. Companies should seriously tackle abusive login attempts by locking or disabling user and device support accounts after a reasonable number of invalid log in

³³ <http://www.forbrukerradet.no/terms-and-conditions-word-by-word>

³⁴ A large number of apps demand access to consumers' private information such as location, contacts and text messages; yet many of them do not fully realize it <https://www.youtube.com/watch?v=xYZtHIPktQg>

³⁵ See <https://ec.europa.eu/digital-single-market/en/news/green-paper-mobile-health-mhealth>

attempts. Examples in this sense can come from other sectors such as banking and e-commerce, which could request a few extra security steps before granting the authorization.

Importantly, security safeguards should concern the whole ecosystem, namely include the network used to transfer health data to avoid any data interception. Researchers have already started to investigate this crucial aspect³⁶. Yet further studies are necessary to find valid encryption solutions that guarantee the best confidentiality, integrity, and authenticity of users' health information. At the same time this is not about deteriorating the overall network performance and/or discouraging the use of these solutions.

6. Different apps, different users

All apps are not equal. One example is clinical decision support apps that are designed to complement healthcare professionals' expertise when diagnosing or treating patients. These apps are intentionally made for clinicians with the medical training needed to interpret the information correctly. Decision support apps may not be reader-friendly or easy to use for consumers seeking information about their condition.

Mobile health users have different profiles and apps should be labelled accordingly to ensure they are used properly. When using a mhealth tool, end users should be able to identify if further support is necessary. Accordingly, developers should clearly specify it and indicate it in the initial terms and conditions.

7. There is no mobile health without internet access & digital literacy

European consumers currently face a number of inequalities related to healthcare financing and infrastructure and available treatments³⁷. Inequalities may run deeper as the uptake of mHealth highly depends on internet availability, which is high in some EU countries but still emerging in others such as Bulgaria and Portugal.³⁸

Although mHealth could connect patients in rural and remote areas with health information, advice and possibly treatment, **17% of the rural EU population still do not have fixed broadband network available in their area.**³⁹ The estimated savings of remote patient monitoring

How are consumers connected?

22% of EU citizens have never used the internet.

Only **36%** of EU citizens accessed internet through a mobile device in 2012, according to the EU Commission.

³⁶ <http://www.ncbi.nlm.nih.gov/pubmed/23624056>

³⁷ http://ec.europa.eu/health/social_determinants/docs/report_healthinequalities_swd_2013_328_en.pdf

³⁸ Special Eurobarometer 381 E-communications household survey June 2012. Reported in the European Commission's Green Paper on mHealth

³⁹ <https://ec.europa.eu/digital-agenda/node/1505> Statistics from the video shown on this page.

should be tempered with the investment needed to ensure internet coverage and mobile devices.

Mobile health puts consumers' health in their own hands. For this reason, consumers' health literacy is crucial to make mHealth successful.

However, health literacy in the EU does not score highly with almost 1 in 2 (47%) survey respondents having limited health literacy⁴⁰. The advent of mHealth complicates this situation when we consider that **only 51% of EU citizen have medium-high internet skills**⁴¹.

Consumers using mHealth are responsible not only for operating these new technologies such as receiving a reminder via an app, but also managing the interface between themselves and mobile devices such as taking or submitting measurements through the app.

Digital literacy is essential to tap into the potential advantages of mHealth. **Older people in particular have lower digital literacy, yet they could benefit the most from mHealth** that is delivered to their hand-held device and tailored to their health needs.

Healthcare professionals play a crucial role for the deployment and the effectiveness of these solutions. Because doctors and general practitioners must build up consumers' confidence in using new technology, their professional developments have to include ad hoc training in mhealth.

Each EU Member State should strive to scale up mHealth in areas where it can be beneficial to health outcomes and health systems. National strategies should specifically address the needs of people with limited internet access (i.e. rural and remote areas, low income, etc.) and/or low digital literacy.

7.1. Consumers engagement in the development of mhealth tools

Consumers are the end-users of mhealth and therefore developing a tool that is easy to use and meet their requirements of safety and security is crucial for the success of mhealth. Involving them during the development would certainly increase the friendliness of the tools as well as the general trust towards mhealth. Similarly, also healthcare professionals should be included in the development, as this would increase the general reliability of information and consequently the general confidence on these tools. This would be particularly the cases of mhealth tools that concern the relation and the interaction between doctors and patients, which have to meet both the expectations and the needs of both actors.

⁴⁰ HLS-EU consortium (2012): comparative report of health literacy in eight EU Member States. The European Health Literacy Survey HLS-EU, online publication: <http://www.health-literacy.eu>

⁴¹ <https://ec.europa.eu/digital-agenda/node/1505> Statistics from the video shown on this page.

Conclusion

Mobile health has the potential to facilitate consumers' access to healthcare, empower them and therefore improve their health.

However, we need further studies to assess the impact of mhealth on healthcare systems. On top of that, a **proper regulation** is necessary to ensure safety, security and quality of information.

A clear and comprehensive legal framework has to ensure reliability of all mhealth solutions – and not just those falling under the definition of medical device - , in terms of quality and data protection and clear rules on liability when things go wrong.

Consumers' trust is fundamental to boost the potential of mhealth. Thus consumers must be reassured about the collection, the treatment and the storage of their health data. To ensure that, mhealth apps should have **privacy by design default settings** and collect no more data than those required for their functioning. At the same time, terms and conditions have to be easily understandable for all consumers.

Policy makers should consider also **additional security safeguards** such as encryption and user authentication to strengthen the particular category of health data.

There has to be a **clear legal responsibility and accountability** for the design, supply and functioning of mhealth apps all along the life cycle of the device, as well as defined consumers redress mechanism for faulty products.

Finally, EU policy-makers need to ensure that mhealth does not create greater divide between EU member states and among citizens. To do that and avoid that mhealth turns into a market-driven consumer alternative for the most educated consumers, **national health policies have to incorporate mhealth** and promote it among all consumers and healthcare professionals.

END