AN EXPLORATORY EMPIRICAL ANALYSIS OF THE QUALITY OF MOBILE HEALTH APPS

Aude Cabrera[1], Mayoni Ranasinghe[1,a] , Cedric Frossard[1], Nicolas Postel-Vinay[2,a] and Celia Boyer[1,b]
[a]*MD*
[b]*Dr*
[1]*Health On the Net Foundation, 2 chemin du Petit-Bel Air, 1225 Chêne-Bourg, Switzerland*
[2]*Unité d'hypertension artérielle. Hôpital Européen Georges Pompidou, 20, rue Leblanc 75015 Paris - France*

ABSTRACT

Introduction: Owning a smartphone is now almost a given, and with smartphone use comes the benefit of access to a large pool of apps on every topic conceivable, including health. So, it is not surprising that mHealth apps development is on the rise, as is the use of mHealth apps. However, unlike apps intended for other purposes, the use of mHealth apps carry, not only the advantage of improved health but also the burdens of potential misuse, misleading content and possible security breach of personal data. In this paper, we attempt to evaluate the possible hazards of some of the most popular mHealth apps in app stores from France.
Objectives: To (1) examine the top 10 most downloaded health apps in term of security and transparency of content (2) identify the trends of the most downloaded apps (3) to assess the applicability of the mHONcode guidelines to identify main issues on health apps (4) to describe the still main risks of health apps and (5) to propose basic rules to overcome them.
Results: As expected, the 10 apps displayed varying degrees of quality and trustworthiness or lack thereof. Only 20% of the apps disclose the editorial team and the funding source. 80% of the apps use tracking tools such as analytics, crash reporting without prior consent or before the consent. 2 out of 10 apps did not used a https web address for health content and advertisement display. One app activates the location functionality without any justification in the app.
Conclusion
As was the case for online health information more than 2 decades ago, the lack of uniformity of the trustworthiness of mHealth apps is worrying and could have some serious public health concerns. And just like the HONcode was required then, the mHONcode is required now to ensure the regulation of health apps, thus providing the end-user with trustworthy and quality tools to help in the management and maintenance of their healthcare.

KEYWORDS

Mobile Applications, mHealth, Certification, Quality, Code of Conduct

1. INTRODUCTION

Health On the Net Foundation (HON) is a non-governmental organization in special relation with WHO (World Health Organization). It is the oldest online health information standardizing body and was founded in 1995 in Geneva, Switzerland. The Health On the Net Code of Conduct (HONcode), a set of 8 principles used to standardize online health information has been in use for over 20 years, for health websites. The mHONcode is the new code of conduct of HON, with guidelines adapted to mobile health apps. Apps owners voluntarily request the mHONcode certification, then their application is evaluated on the one hand on reliability by a medical expert and on the other hand on safety by a member of our IT team. Before any evaluation, a contribution is requested, since the processes require between 3 and 5 days of work by experts. This does not in any way guarantee that the certification will be obtained, the application needs to be fully compliant to be certified.

ISBN: 978-989-8533-94-4 © 2019

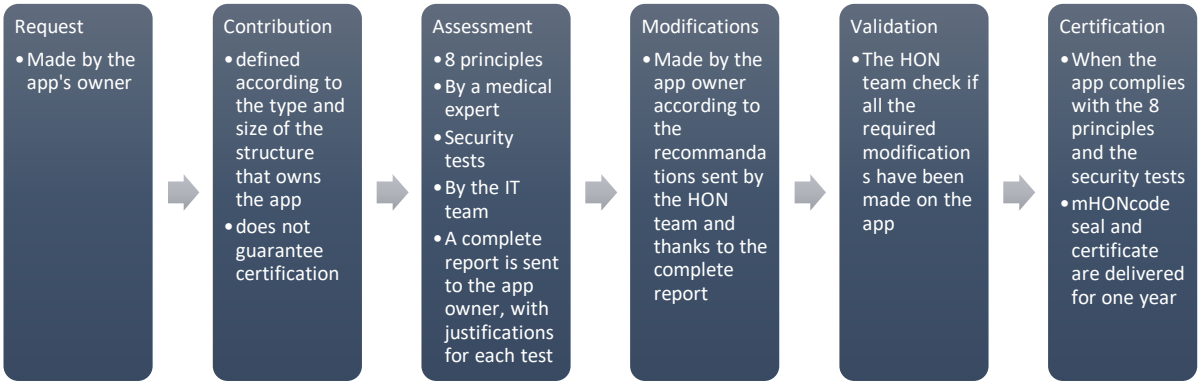

Figure 1. Process of the mHONcode certification

The former European Commissioner for Health Tonio Borg said in 2014 "mHealth has a great potential to empower citizens to manage their health and stay healthy longer, to trigger greater quality of care and comfort for patients, and to assist health professionals in their work. As such, exploring mHealth solutions can contribute to modern, efficient and sustainable health systems"[1]. Mr Borg's visionary comment was indeed true. However, as is the case with most things, there are always pros and cons. The pros are immense, with mHealth having the potential to greatly impact population health, but the cons are that there are no indicators to allow the public to discern trustworthy apps from the crowd.

So how popular are mHealth apps? Where do we stand today in 2019 in terms of mHealth adoption and usage? In 2017, 325,000 health apps were available in all major app stores (Google Play, Apple App, Windows Phone, Amazon App and Blackberry world), this equates to 3.7 billion of downloads (Research 2 Guidance, 2017). Between 2016 and 2017, 78,000 health apps were added to Google Play and Apple App stores (Research 2 Guidance, 2018). A systematic review conducted by McKay (2018) has shown the lack of one best practice approach to evaluate mobile health apps amongst the scientific community. In this huge market, how would the general public, without any medical knowledge or a health care provider recommending a health app, be able to gauge the trustworthiness, accuracy and security of an app to use or recommend? What are the criteria a mHealth app should fulfill to be available for download in the app stores? Are the security of health and personal data and the transparency of information considered a major issue to be considered in the mHealth arena? Are these issues taken seriously by mHealth developers and stakeholders commissioning the developments on their behalf?

Carroll et al. have shown that younger persons (18-44years) with a higher education (college graduate or higher) have a higher likelihood of adopting health apps than the ones aged 45-65+years. Furthermore, they highlighted the role of mobile phone health apps as a health promotion tool to change lifestyle behaviors (perform physical activity, change diet and lose weight). mHealth apps are in full expansion in the healthcare domain (Wellness. Education, Prevention, and Care) including in their use by the general public, however the regulation measures for these apps have not kept up.

The numbers are worrying: a study shows that 66% of the health apps certified as clinically safe by the UK NHS apps Library were in fact, sending identifying information over the internet without encryption and disclosure [Huckvale 2015 a]. Huckvale 2015 b, in another paper, demonstrates that 67% of the insulin dose calculator apps assessed provided inappropriate dosage recommendation. Plante in 2016 showed that a blood pressure measuring app produced false measurements, and this app had been downloaded 150,000 times. These are only a few examples. Wisniewski 2019 highlights that apps based on six diseases (depression, schizophrenia, addiction, hypertension, diabetes, and anxiety) provide questionable content or unsupported claims. Recent scientific publications have shown that sharing of user data is routine and yet far from transparent despite the introduction of the European Union General Data Protection Regulation (GDPR) in 2018, preventing the user from making an informed choice regarding the transmission of their data to third parties [Huckvale 2019 and Grundy 2019]. So, the ubiquity of smartphones, tablets, sensors and similar smart devices means that huge volumes of data concerning health and personal data are being harvested and processed without even the users' knowledge.

[1] http://europa.eu/rapid/press-release_IP-14-394_en.htm

Amid the massive choice available to the public along with the accompanying risks, no real, sustainable solution currently exists to help differentiate the trustworthy from the non-trustworthy. Additionally, knowing that 23% of the digital health marketers are non-healthcare professionals [Research 2 Guidance, 2017], how can users identify reliable applications?

2. OBJECTIVES

In this article, we observe the top 10 most downloaded health apps available on Google Play and Apple Stores in France to understand their offers and behaviors in terms of security and transparency of content. Through this first step, we categorize the most downloaded apps in France in terms of functionalities (Table 1). These 10 health apps are judged according to the mHONcode guidelines (Table 3) to identify the main issues on health apps. The idea is to understand if these guidelines are applicable to the commonly used health apps and how scalable it is to accommodate the growing number of apps, while considering the heterogeneity of the apps and the time spent on each of them. Based on the assessment, the main risks of the 10 health apps are identified and solutions are proposed to overcome them.

Given the increasing focus of data privacy breach or issues in the general press, apps making unsupported claims and the proliferation of health apps on the market, the understanding of these research questions is relevant and timely to guide healthcare providers, the public and stakeholders to improve health apps in terms of data privacy and content transparency and honesty.

3. METHODS

HON chose the 10 most downloaded free health apps in the two major stores Google Play & Apple with the limitation of the country in the URL of the stores being France, without discrimination of language, mission, functionalities and rating. None of these apps has voluntarily required the certification or been HONcode certified now. As we wanted to test if the GDPR[2] was adopted by apps after this new European regulation came into force across the European Union on 25th May 2018, we decided to opt and select the country France. The aim was then to have a representative sample of applications without any further sorting other than choosing the most downloaded applications by users, to obtain results that were limited but representative of the current market of mobile applications as in line with the other publications described below. As the top 10 apps is different for either the Apple Store or the Google Play Store, and also because this list changes from day to day, we selected the 10 most downloaded apps between the 2 stores, on May 24th 2019. We also reported the number and the score of ratings as users could base their choice on such criteria. All this information can be found in Tables 1 and 2.

Table 1. Positions, number of downloads for the 10 selected apps on May 24th, 2019, in France

Application	Versions	Owner	Category	Apple store's positions	GooglePlay store's positions	Downloads in the GooglePlay store
Doctolib	iOS 3.2.1 Android 3.1.9	Doctolib	Appointment booking	#1 Medical	#1 Medical	>1 million
Grossesse +	iOS 5.4 Android 5.2	Philips / Health & Parenting	Pregnancy	#2 Medical	#1 Parents	>10 million
Qare	iOS 1.7.65 Android 1.8.85	Qare SAS	Online consultation	#3 Medical	#2 Medical	>100 000
Staying Alive	iOS 6.1.3 Android 6.2.2	AEDMAP	Cartography	#4 Medical	#5 Medical	>500 000
Sauv Life	iOS 2.5.4 Android 2.3.4	Association S.A.U.V.	Cartography	#5 Medical	#7 Medical	>100 000

[2] https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/

We Moms	iOS 2.14.17 Android 2.61.07	Globalia SAS	Forum	#6 Medical	#9 Parents	>500 000
Mon Ovulation	iOS 1.4.3 Android 2.7.1	Doctissimo / TF1 / Lagardère	Fertility	#7 Medical	#27 Medical	>500 000
Livi	iOS 3.0.6 Android 3.0.5	Digital Medical Supply France	Online Consultation	#8 Medical	#4 Medical	>100 000
Bébé +	iOS 1.9.4 Android 1.8.4	Philips / Health & Parenting	Baby's health	#9 Medical	#6 Parents	>500 000
Ma Grossess	iOS 2.6 Android 2.9.0	Doctissimo / TF1 / Lagardère	Pregnancy	#10 Medical	#12 Medical	>1 million

Table 2. Ratings and number of ratings for the 10 selected apps on May 24th, 2019

Application	Users's rating for GooglePlay	Numbers of rating For Google Play	User's rating For Apple Store	Numbers of rating for Apple Store
Doctolib	**4.8 / 5**	29 000	**4.8 / 5**	11 300
Grossesse +	**4.6 / 5**	384 000	**4.7 / 5**	5 800
Qare	**4.7 / 5**	567	**4.8 / 5**	2 000
Staying Alive	**4.1 / 5**	2 000	**4.2 / 5**	2
Sauv Life	**3.9 / 5**	786	**4.3 / 5**	297
We Moms	**4.6 / 5**	9 000	**4.7 / 5**	129
Mon Ovulation	**4.2 / 5**	4 000	**3.5 / 5**	6
Livi	**4.5 / 5**	877	**4.9 / 5**	2 700
Bébé +	**4.5 / 5**	29 000	**4.7 / 5**	1 300
Ma Grossesse	**4.3 / 5**	32 000	**4.3 / 5**	34

10 applications, French and English language-based health-related mobile apps were assessed by two senior expert members of the HON team, following the new guidelines for app certification: the mHONcode (Table 3). This new code of conduct also includes two security tests: an automated test for detection of weakness and vulnerabilities and a test about privacy & encryption which analyze the application's network, they can be found at the end of Table 3. Thus, 10 apps were manually checked by the IT team regarding the traffic of the data sent by apps on the Internet through differential traffic and network analysis. This allowed us to understand (1) the data sharing practice of the apps, how the personal data are transmitted (via a secure link SSL, and how the password and login are transmitted – encrypted or not) and (2) to which third parties personal data are sent with consent or not. These analyses have been done using Mitmproxy, a free open source interactive https proxy[3] allowing to be in between of the app transmission of data over the Internet and the phone. In addition, the Mobile App Security Test[4], free product by ImmuniWeb, has been used to scan the code. For Android the APK or the Google play link to upload the code was used, while for iOS an IPA archive was mandatory. This free product provides automated tests regarding six different test types: Static Application Security Testing (SAST); Dynamic Application Security Testing (DAST); Behavior Testing for malicious functionality and privacy; Software Composition Analysis; Mobile Application Outgoing Traffic and Mobile App External Communications. This product was selected as it provides a complete and easy to understand report and is free of charge, with an API or a web version. The results of these tests were analyzed by our team and major ones are reported in the results section. The 10 apps were downloaded to a HUAWEI P20 Android version 9.0.0, Android 8.1.0 and an iPhone 8 iOS version 12.2.

[3] https://mitmproxy.org/
[4] https://www.immuniweb.com/mobile/#about

Table 3. Presentation of the 8 principles of the mHONcode

Principles & Security Tests	**Description**	**Examples of questions**
1- Authority	Details about the editorial team, and the app team are clearly disclosed.	Are the name and qualifications of the editorial manager and the qualifications of writers provided? Who is in charge/responsible for the app?
2- Complementarity	Clear mention of the limitations of the app which does not replace the doctor-patient relationship.	Do you have a statement indicating that the information provided on the application is intended to encourage, not replace, direct relationships between the patient and health professionals?
3- Confidentiality	Statement explaining all legal requirements regarding the confidentiality of personal data.	Does the GPDR apply to your service? Is consent to data collection required for the use of the application? Are data transmitted to third parties?
4- Validity	App & all health and legal content have a 'last updated' date.	Does the medical, legal content and app have a last updated date?
5- Justifiability & Objectivity	Health information has references, is complete, and provided in an objective manner.	If app has services with formulae calculating dosage or health scores, are the references / scientific bases of these formulae given? If app has medical content, are the references given and medical information provided in an objective and balanced manner?
6- User's practice	The app is user friendly, its mission is clear, and the team is easily reachable.	What is the mission and audience of the application? Are there any instructions for use? Is a support contact address accessible or is it possible to leave a feedback?
7- Financial disclosure	All funding sources and paid services are identified and transparent.	What are the source(s) of funding? If the application needs an integrated purchase for its use, are there any general conditions available on this subject in the app? Is there a declaration of disclosure of links of interest for health professionals providing content or advice?
8- Advertisement policy	All ads are identified and clearly separated from the content.	If the application displays advertising, is it clearly identified as such and is there a viewable advertising policy on the application? If there aren't ads in the app, does a disclaimer indicate that there is none?

4. RESULTS

Various subjects were covered by the apps assessed: pregnancy, fertility, online consultation, cartography, baby's health, forum. The audience of these apps was the public. Regarding the new code of conduct and especially the 8 principles, the Table 4 shows for each application if it respects each principle. The symbol ✗ means that the principle is not present in the app, while ✓ means that the principle is respected by the app, and **NA** means that the principle doesn't apply to the app. For some principles, we separated the results to be more precise, the signification of each initial is indicated below.

Table 4. Compliance with each principle for each application

Principles / Apps	**1 Authority**	**2 Complementarity**	**3 Confidentiality**		**4 Validity (Dates)**			**5 Justifiability Objectivity**		**6 User's practice**				**7 Financial disclosure**	**8 Advertisement policy**	
			Policy	*Consent*	*M*	*L*	*A*	*R*	*O*	*M*	*A*	*I*	*S*		*Policy*	*Identi-fication*
Doctolib	✗	**NA**	✗	✗	**NA**	✗	✗	**NA**	**NA**	✗	✗	✗	✗	✗	✗	**NA**
Grossesse+	✗	✓	✓	✗	✗	✓	✗	✗	✓	✗	✓	✓	✓	✗	✗	✗
Qare	✓	✓	✓	✗	✗	✓	✗	**NA**	**NA**	✓	✗	✓	✓	✗	✗	**NA**
Staying Alive	✓	✓	✓	✗	**NA**	✗	✗	**NA**	**NA**	✗	✗	✓	✓	✓	✓	**NA**

Sauv Life	×	**NA**	✓	×	**NA**	×	×	**NA**	**NA**	✓	✓	×	×	×	×	**NA**
We Moms	×	✓	✓	✓	×	✓	×	×	✓	✓	✓	✓	×	×	✓	✓
Mon Ovulation	×	×	×	×	×	✓	×	×	✓	×	✓	×	✓	×	×	×
Livi	×	✓	✓	✓	**NA**	✓	×	**NA**	**NA**	✓	✓	✓	✓	×	×	**NA**
Bébé +	×	✓	✓	×	×	✓	×	×	✓	✓	✓	✓	✓	×	×	×
Ma Grossesse	×	×	×	×	×	✓	×	×	✓	×	✓	×	✓	×	×	×

Principle 4 Validity: M: Medical content / L: Legal content / A: Application
Principle 5 Justifiability & Objectivity: R: References / O: Objectivity
Principle 6 User's practice: MA: Mission & Audience / I: Instructions / S: Support

Regarding the automated code and privacy and encryption tests, 2 out of 10 apps are not using an https web address, a secure internet connection with SSL (Secure Socket Layer) for the transfer of health content, to access server type as content delivery network (to display images) as well as for displaying ads banners. The SSL certificate authenticate the identity of the organization delivering the service, ensure confidentiality and integrity of the content as information exchange cannot be intercepted and modified. So, personal data such as IP or health domain of interest could be intercepted by malwares.

One app is transmitting login and password information clearly displayed in the URL while the URL is using a secure protocol (HTTPS). The security whole in this case could be at the level of the storage of logs, where the login and password information are stored and potentially vulnerable to attacks.

Finally, 6 apps out of 10 use tracking such as analytics, crash reporting and others, transmitting personal data regarding to the GDPR without any prior consent of the user. 2 apps request prior consent but are already using tracking information before this explicit consent. Only 2 of the 10 apps required clear consent from the user at the time of first use, without clicking in the checkbox, users don't have access to any functionality of the application. 5 apps display a mention indicating that, by continuing to use the app, the user accepts the terms of conditions and confidentiality policy. Furthermore, 8 of the 10 assessed apps transmit data to third parties such as advertisement partners or tracking reporting or analytics tools.

During the analysis of the code via Immuniweb, we identified the following permission used by the apps such as camera (7 apps), microphone (4), location (7), phone (5), calendar (5), ssd storage or media storage (8), contact (1), Bluetooth (none but 4 apps declared in the code the need to use it), accelerometer (none but 5 apps declared in the code the need to use it). One app did ask the consent for using the location information, however this functionality was not used in the app so the demand of this usage was unjustified. Such behavior is infringing the GDPR.

8 out of 10 app declared the usage of above phone information in the code, without really using it. The habit of declaring the usage without using it, is not a good one as it is a potential security flaw for android versions above 6 Marshmallow used by 25% of android smartphone users[5].

In 90% of cases, the iOS and Android versions do not declare the same need of phone functionalities.

One app with the Android version was using the calendar of the phone without requesting permission, this has implied the crash of the app induced by Android OS as explicit permission was not granted.

5. DISCUSSION

After the assessment of the 10 most downloaded apps in France, we found major issues with the transparency, honesty and security of these apps.

Most of these apps didn't have any information about who is in charge/responsible for the app or the editorial team (Principle 1). Only 2/10 apps offering medical/health content mentioned the editorial process responsible, the authors or the process of information creation. None of the apps mentioned the sources of the health content nor the scientific background for the information (Principle 5). These apps are downloaded from 500,000 times to 10 million times; if the content is not verified, trustworthy, how can we not be alarmed by the major public health problem they are likely to represent?

Another issue presented in 2/10 apps is the missing statement that the health content or services on the app should not be used as a replacement of medical professional's advice. (Principle 2).

[5] https://developer.android.com/about/dashboards/

Additionally, particularly related to medical content but also legal content, is the date of the last update of the content (Principle 4). None of the 10 applications evaluated contained a creation date or last update of health information. This means that users' access health content, in most cases without references or authors, but also without knowing if it is still relevant. This creates a certain problem: the user bases his or her health decisions on potentially obsolete content. And yet it is well known that health and medical information is constantly and rapidly evolving.

Regarding the financial disclosure (Principle 7) only 1 of the 10 apps provided specific information on its funding.

Regarding advertising (Principle 8), 1 apps out of 10 displayed advertising inserts when used, but advertising policies on the subject are not well described and the ads in question are very poorly identified, or even very intrusive for one of the app.

Out of all, the 8 principles, the user experience (Principle 6) was the best represented for the 10 apps we evaluated. Most of them offer help, tutorials or a FAQ section to assist the user in using the application. 7 of them have easy access to a support address.

From a data privacy point of view, 8 out of 10 apps have a confidentiality policy specific to their app. 2/10 apps, with over one million downloads, with a service requiring registration of personal and identifiable information, did not have any reference to confidentiality or GDPR while having a very high rating score by the users.

In addition, the practice is different when examining the traffic of the data, 8 out of the 10 transmit personal data without prior consent or securely. This is a danger to users' data, users cannot be aware of such misuse. We could question if the developer team is aware of the good behaviour in terms of security and GDPR regulation. This is infringing the GDPR while these apps should strictly respect it unless penalties of 2% annual global turnover should apply. Probably this is due to the lack of policy enforcement and owner willingness.

The rating score given by end users is not reflecting the behaviour of the apps in term of transparency, ethics and security, in fact, it is even nearly the opposite. This was also identified by Wisniewski, which suggest the usage of the last update as a selection feature. In our case, this feature was only present. The issues identified in this article could be very easily corrected but concern the editorial process and the IT team developing the app.

6. LIMITATIONS

This study has limitations. The main one is that we only assessed 10 applications, the most downloaded in France. Nevertheless, these apps are representative of the common behavior of apps, as probably these apps have more potential to be in line with regulation such as the GDPR and good practice as all are owned by well-established organizations. So, the results presented, and the proportions should be read as indicators of the frequency of the behavior rather than definitive statistics.

HON is proposing new guidelines on mobile apps and have assessed these apps regarding these guidelines. This can be a bias; however, we equally assessed all the apps, by two senior HONcode experts.

The app behavior and services offered is sometimes based on the language of the phone which means that the service assessed differs so the review outcome can be different. This occurred on one application, LIVI, where when detected in English the service differed totally and required an address in UK, while when having a French version, even if we are in Switzerland, the service asked for the French security card or for online paid teleconsultation service.

Finally, with other studies analyzing the traffic of apps, this can only represent a snapshot at a given time.

7. CONCLUSION

mHealth is a huge market which provides users the opportunity to have better health and healthcare quality. Health apps support citizen's empowerment through self-management, health promotion, disease prevention, providing personalized health advice and care. However, the risks involved must be considered; the rapid development of the mHealth sector raises concerns about the potential risk of health functions apps providing transmission of health data, the capture of these data via sensors, self-diagnoses, disease management or diagnosis and appropriate processing of the data collected. Since mHealth solutions and devices can collect

large quantities of personal information, including personal health information (e.g. data stored by the user on the device and data from different sensors, including location) and processes them.

The major difficulty for not only general users but also for health professionals who could recommend apps, is to discern trustworthy apps from the large pool of apps out there and our list assessment confirms this challenge.

Users, with this new technology in their hands, have direct access to medical and health information, with no need to take an appointment, straight from their pocket, which of course represents massive advancement in healthcare but also a real danger, if the displayed information is not reliable and if they believe that it can replace a consultation with a health professional.

As other studies, our study based on the 10 most downloaded mobile apps in France has shown clearly that mHealth apps, are sharing data which is far from transparent [Huckvale 2019 and Grundy 2019]. The non-respect of the 8 mHealth HONcode guidelines and issues in terms of privacy or security identified could be easily overcome with guidance to the developing team and decision from the owners of these apps. Given that there is no control, why would app developers decide to conform to strict editorial processes such as security, honesty and transparency which would cost more without short-term benefit in terms of number of downloads or ranking?

Although, even if only 10 apps were used in this study, it should be remembered that the 10 chosen were the most popular and thus, a representation of what the public downloads and uses.

mHealth apps are excellent ways to improve your health, in a fast, fun and accessible way, but only if they are reliable. Otherwise, which seems to be confirmed on this panel of apps, they represent a real public health danger, which can be overcome only with the commitment of the owners of these apps which the HON Foundation will try to address through its new code of conduct, the mHONcode.

ACKNOWLEDGEMENT

We thank the app owners who trust us and helped us finalize the HONcode principles.

REFERENCES

Boyer, C., & Geissbuhler, A. et al. 2007. Health on the Net Foundation: assessing the quality of health web pages all over the world. In *Medinfo 2007: Proceedings of the 12th World Congress on Health (Medical) Informatics; Building Sustainable Health Systems* (p. 1017).

Carroll, J. K., et al, 2017. Who uses mobile phone health apps and does use matter? A secondary data analytics approach. *Journal of medical Internet research*, *19*(4), e125.

Grundy, Q., Chiu, K., Held, F., Continella, A., Bero, L., & Holz, R. 2019. Data sharing practices of medicines related apps and the mobile ecosystem: traffic, content, and network analysis. *bmj*, *364*, l920.

Huckvale, K., et al, 2015 a. Unaddressed privacy risks in accredited health and wellness apps: a cross-sectional systematic assessment. *BMC medicine* Vol. 13: 214

Huckvale, K., Adomaviciute, S., et al, 2015 b. Smartphone apps for calculating insulin dose: a systematic assessment. *BMC medicine*, *13*(1), 106.

Huckvale, K., Torous, J., & Larsen, M. E. 2019. Assessment of the data sharing and privacy practices of smartphone apps for depression and smoking cessation. *JAMA network open*, *2*(4), e192542-e192542.

McKay, F. H., et al, 2018. Evaluating mobile phone applications for health behaviour change: a systematic review. *Journal of telemedicine and telecare*, *24*(1), pp. 22-30.

Plante, T. B., Urrea, B., et al, 2016. Validation of the instant blood pressure smartphone app. *JAMA internal medicine*, *176*(5), 700-702.

Ranasinghe, M., Cabrera, A., Postel-Vinay, N., & Boyer, C. 2018. Transparency and Quality of Health Apps: The HON Approach. *Studies in health technology and informatics*, *247*, 656-660.

Research 2 Guidance, 2017. *mHealth App Economics 2017/2018 Current Status and Future Trends in Mobile Health* Research2Guidance report. USA, pp 10. URL: https://research2guidance.com/product/mhealth-economics-2017-current-status-and-future-trends-in-mobile-health/ [Accessed May 2019]

Wisniewski, H., Liu, G., Henson, P., Vaidyam, A., Hajratalli, N. K., Onnela, J. P., & Torous, J. (2019). Understanding the quality, effectiveness and attributes of top-rated smartphone health apps. *Evidence-based mental health*, *22*(1), 4-9.