27 Quality and Safety of Health Mobile Applications: Are They an Issue?

Célia Boyer

Learning Objectives

- 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 carries, 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 chapter, we present different initiatives involved in finding solutions to limit the issue of variability of the quality of health apps. We introduce how the mHONcode can be used to evaluate the possible hazards that you can find in some of the most popular mHealth apps in app stores. The mHONcode criteria will help you to identify and assess the trustworthiness of health apps, thus providing the end-user with trustworthy and quality tools to help in the management and maintenance of their healthcare.

Key Terms

- Mobile applications
- mHealth
- Trustworthiness
- Certification
- Quality
- Code of Conduct

Introduction

On the Web today, it is difficult to determine what information is valuable and what is useless. One of the concerns is the growing number of health websites of doubtful quality brought about by the popularity of the Internet. However, between 2012 and 2020, the number of existing websites increased by 180%, to nearly 1.8 billion in 2020, according to Internet Live Stats.[1] Health websites compete with health applications for smartphones and pose multiple dangers in the form of the quality of health content as well as the issues of confidentiality and security of private data.

It is estimated that over 200 health apps worldwide are being added each day to the top app stores, with over 325,000 health apps available in 2017 alone and downloaded 3.6 billion times and designed by 84,000 developers [1, 2]. Despite the short period of time, there is already evidence of health apps playing a positive role in both patient outcomes and the costs of care.

According to a survey conducted in 2018 (Day S. Zweig M.), both patients and physicians

[1] Internet Live Stats (2020). Total number of websites. URL: http://www.internetlivestats.com/total-number-of-websites/#trend [Accessed 05 June 2020].

C. Boyer (✉)
Health on the Net Foundation, Geneva, Switzerland

U. H. Hübner et al. (eds.), *Nursing Informatics*, Health Informatics,
https://doi.org/10.1007/978-3-030-91237-6_27

are ready for increased digital engagement. Approximately 85% of health apps in the market today are for wellness, designed to be used primarily by the consumer, and the remaining 15% are medical, designed to be used by physicians [3].

e-Health connects the companies that develop applications and the healthcare consumers who use them. Two major problems arise in this "digital care:" the reliability of the application and data security [4].

In the midst of this huge e-health market, how can we distinguish reliable, high-quality, and secure applications from those that may represent a danger to users and thus to public health?

Healthcare consumers continue to show strong use of digital technology, with numbers rising each year. In fact, the adoption of digital health technology is at its highest rate ever—with 89% of respondents using at least one digital health tool in 2018 [5]. Thus, it is very important that the quality of this technology be optimum, which is unfortunately not always the case. For example, some applications allow people to measure their blood pressure by placing the pulp of their finger on the camera of their smartphone. Unfortunately, the figures displayed are not reliable, and users are misled by the results of the apps. The need for an evaluation of the reliability and veracity of health applications is real, and many opinions agree on this matter.

The other point identified is that of the security of the application and of the data that the user transmits, sometimes without being aware of it, via the application, and which is sometimes shared with third parties without his consent [6]. The most blatant example is the one that appeared in the Wall Street Journal in February 2019 [7], revealing that several applications had sent the data collected to Facebook without authorization. Thus, a second, non-negligible need emerges—that of the user to be able to ensure that their data is not shared without their consent and that they are able to use the app safely without doubt of breach of privacy.

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."[2] 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. A systematic review conducted by McKay [8] has shown the lack of a uniform 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?

Carroll et al. [9] have shown that younger persons (18–44 years) 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 at the same pace.

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 [10]. Huckvale et al. [11], in another paper, demonstrate that 67% of the insulin dose calculator apps assessed provided inappropriate dosage recommendations. Plante in 2016 [12] showed that a blood pressure measuring app produced false measure-

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

ments, and this app had been downloaded 150,000 times. These are only a few examples. Wisniewski et al. [13] highlight that apps based on six diseases (depression, schizophrenia, addiction, hypertension, diabetes, and anxiety) provide questionable content or unsupported claims. 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 [14, 15]. 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.

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 [2], how can users identify reliable applications? 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?

Approaches to Assess Health Apps

The rapid development of the mHealth sector raises concerns about the potential risk of health functions apps providing transmission of health data, capture of health data via sensors, self-diagnoses, disease management or diagnosis and appropriate processing of the data collected through apps or solutions 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. Apps pose a new challenge that cannot be solved as we did for health content websites, mainly because of several reasons: (a) all the data is visible in health websites as it is part of the content and so it is easy to check the production process of the content; whereas in an app, the algorithms used to analyze the data are kept secret and not disclosed (industrial secrets); the privacy and security of transmission and storage is very difficult to test and assess (b) apps play the role of a "medical device" even if theoretically they are not which is unlike health websites which do not play a diagnostic role but only an informational role. So, the intrinsic risks posed by apps are totally different from health websites.

Health apps supporting citizen's empowerment through self-management, health promotion and disease prevention, providing personalized health advice and care has become a challenge worldwide [16].

The "annual study on mHealth" suggests that the ubiquity of smartphones, tablets, sensors, wearables, personal trackers, and similar wireless smart devices means that huge volumes of data concerning health, fitness, lifestyle, stress, and sleep are being harvested and processed [16]. This report foresees that in 2020, 551Million users will by then actively (at least once a month) make use of a mHealth app.

The main issue then becomes how to identify the most appropriate, adapted, and trustworthy health app out of hundreds of thousands of similar health apps.

Another major risk of apps is that they work according to a set formula or standardized algorithms, which are relatively unchanged from patient to patient. This then does not allow the capture of the other aspects of clinical diagnosis such as clinical observation or personal medical history of the patient and his/her various signs.

Health apps have to undergo specific accreditation in the USA by the FDA to be categorized as medical devices [17]. So far in Europe, there is no such specific directive for apps except the Code of Conduct on privacy for mobile health apps submitted for approval to the Art 29 Data Protection Working Party [18]. So in Europe, health apps to be labeled as medical devices should respect the Council Directive 93/42/ECC concerning medical devices. This chapter does not address the health apps as medical devices as it is governed by clear regulation.

However, the majority of health apps labeled as non-medical device also provide medical functionalities such as auto-diagnosis and auto-medication. Mobile apps span a wide range of health functions, with potential benefits and risks to public health compounded by the fact that these apps are potentially available to billions of people worldwide. Depending on the type of the app and its intended use, the potential risk will vary and thus, the level of scrutiny given should be proportionate to the risk.

Different initiatives propose solutions to solve the problem of the quality and security of mobile apps. Below in Table 27.1 is a non-exhaustive list of some initiatives, guidelines, rating tools, recommendations, and scale to assess the level of trust of a health app. New approaches are published regularly, such as the THESIS rating tool [19] but the common point of all these approaches is the difficulty to implement them and to be used by health apps developers. The common criteria addressed by these rating tools, labels, or guidelines are the transparency, health reliability, technical consistency, security and privacy disclosure, and usability.

Various organizations worked on the issue of security, data privacy, and other criteria related to quality [20]. However, due to the complexity and liability risks to potentially unidentified issues such as the security issue, the assessment of health apps is at its very early stages. A study highlighted that 66% of the health apps certified as clinically safe and trustworthy by the UK NHS apps Library was in fact sending identifying information over the internet without encryption and without disclosure that the app will do so [10]. This has caused the NHS apps service to close for a while. This study has raised three elements of reflection: the current lack of transparency and responsibility of apps related to data usage, storage, and transmission; what can be evaluated reasonably and sustainably; and the risk that no organization assesses health apps as the risk is too important to miss or not be able to check all the necessary elements to guarantee

Table 27.1 Presentation of several labels and guidelines for health apps monitoring—August 2020

Name	Country	Developer	Functioning	Inventory
NHS apps Library	UK	NHS	Registration needed, fee-based evaluation not disclosed. Criteria of evaluation disclosed[a]	95 apps in the NHS Library[b]
Calidad app salud	Spain	Agencia de Calidad Sanitaria de Andalucia	Free 31 recommendations Assesses design, quality, services, and privacy [10]	20 app assessed, 70 under assessment
Just think app	USA	American Health Information Management Information	Brochure to inform and educate users [11]	Education No implementation
MOBILE APPLICATION RATING SCALE	Australia	Queensland University of Technology	23 questions Grading scale from 1 poor to 5 excellent [12]	Self-evaluation
code of conduct on privacy for mhealth app	EU	European Commission	The Code was issued after a research study in 2014 [8]	No implementation
Good practice guidelines on health apps	FRANCE	French Health National Authority	5 categories: Information to users, health content, security, data usage and technical usage [13]	No implementation
mobile app privacy code of conduct	USA	US Government	Privacy notice to disclose their practice related to data storage and usage [14]	Voluntary Not widely used

[a] https://shorturl.at/juFO0
[b] https://www.nhs.uk/apps-library/

security and accuracy. On the other hand, should we rely only on the current model of user rating proposed by the two majors' apps platforms Google Play and iTunes iOS [21] knowing that apps providing measurement of key indicators such as heart rate Blood Pressure readings are commonly downloaded (up to 2.4 million downloads) and rated well?

With the multitude of health apps available today (more than 260,000 health apps), what can be evaluated reasonably and sustainably?

In addition, to assess too many criteria as identified by the HAS will lead to nearly no assessment because the number of apps being assessed will drastically diminish because of high costs and inefficient practices. Transparency and honesty in the production of the apps will engage developers to disclose what is behind the scene and be responsible for what health app it develops. Not all apps need the same attention as they do not imply the same potential risk to consumers. For example, health apps with calculators and algorithms intended to recommend an action or medications may directly impact the user's health [11].

The mHONcode Certification for Mobile Health Apps

Health On the Net Foundation (HON) is a non-governmental organization based in Geneva and in official relations with the WHO (World Health Organization). HON was created to promote the deployment of useful and reliable health information online and to enable its appropriate and efficient use. HON 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 [22]. Two decades on, the HONcode is the oldest and most valued quality marker for online health information. It is a pragmatic solution that has been adopted by more than 8000 websites. This approach has the aim to help consumers to become more efficient at separating fact from fiction and at evaluating credibility on the Web in practice.

In 1996, the Health On the Net (HON) Foundation established the HONcode (Boyer et al. 1998) by working with health information editors to come to agreement on typical and common good practice criteria for health information online. This approach involves the external evaluation of health Web pages by experts. The HONcode is a set of ethical, honesty, transparency, and quality standards covering various aspects of health websites, including the disclosure of the qualifications of the authors, the funding sources, references, when the content was created and last updated, the privacy policy, and how data is stored. The HONcode motivates health editors to be transparent in the production process. The commitment of a health information provider to implement or comply with the HON code of conduct is shown by the displaying of a quality label (logo or HONcode seal) on the website. Sites first submit a formal application for HONcode certification. The health website is then manually checked to determine whether or not it meets the principles for compliance. Once HON has determined that the site is committed to and respects the HONcode, it can display the HONcode seal. The site is checked on a regular basis to ensure that it is still compliant and that the health editors are respecting their ethical commitment. However, HON relies on the community to report misuse of the label or non-respect of a principle via an online form. The goal of the HONcode is to guide Internet users and patients towards trustworthy health information by certifying health websites that offer content respecting the HONcode principles. The HONcode is dedicated to the upkeep of the quality of health website, so a new set of principles have been adapted and tailored for the mobile health apps: the mHONcode.

The mHONcode is the new code of conduct of HON, with guidelines adapted to mobile health apps [23]. Apps owners voluntarily request the mHONcode certification, and 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 as the application needs to be fully compliant to be certified.

mHONcode Certification and Methodology

The mHONcode is a set of ethical, honesty, transparency, quality, and security standards covering various aspects of health apps, including the disclosure of the qualifications of the authors, the funding sources, references, when the content was created and last updated, what the privacy policy is, and how data is stored and transmitted over the internet (Fig. 27.1). The mHONcode motivates health apps editors to be transparent in the production process and in the way to use user's data. The commitment of a health information provider to implement or comply with the HON code of conduct for health apps is shown by the displaying of a quality label (logo or HONcode seal) on the website.

Certification process: The health app owner voluntarily applies via the HON website for the mHONcode certification. Upon this application, the app is evaluated manually by an expert medical team and a security officer according to the mHON principles and associated published guidelines[3] (Tables 27.2 and 27.3). In order for this evaluation to take place, the health app editor needs to fill in a self-reporting mHONcode ques-

[3] https://www.hon.ch/en/guidelines-mhoncode.html

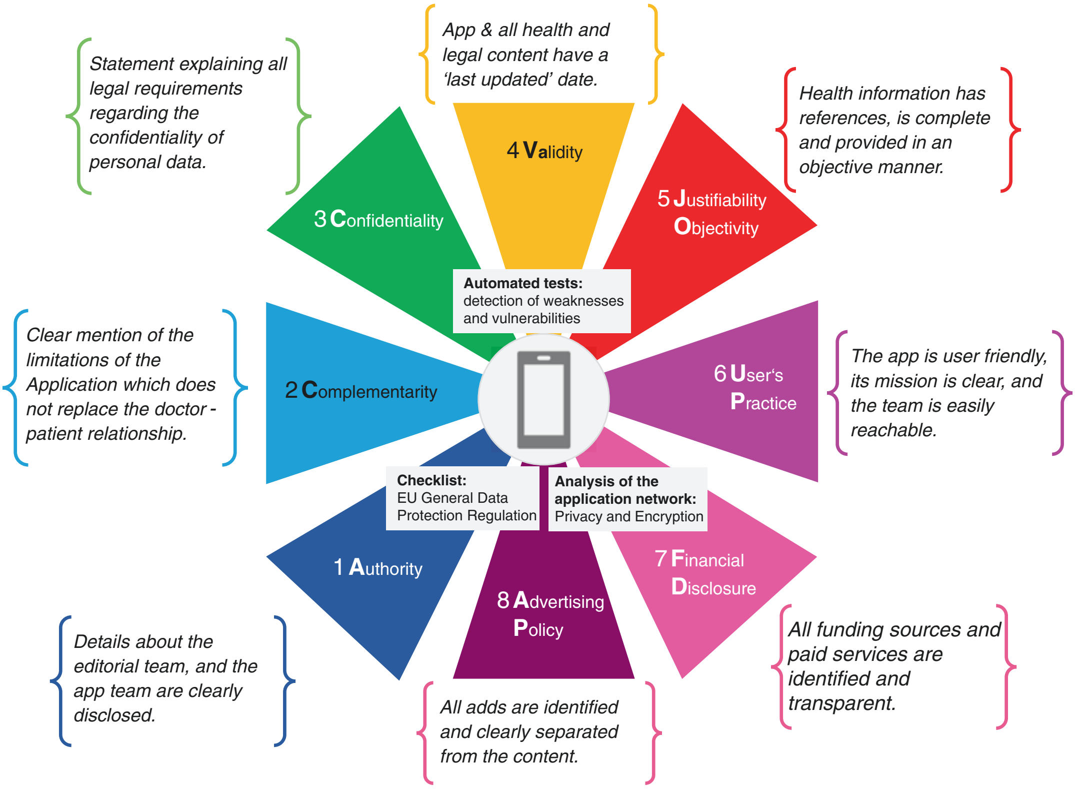
App & all health and legal content have a 'last updated' date.
Statement explaining all legal requirements regarding the confidentiality of personal data.
Health information has references, is complete and provided in an objective manner.
4 Validity
3 Confidentiality
5 Justifiability Objectivity
Automated tests: detection of weaknesses and vulnerabilities
Clear mention of the limitations of the Application which does not replace the doctor - patient relationship.
2 Complementarity
6 User's Practice
The app is user friendly, its mission is clear, and the team is easily reachable.
Checklist: EU General Data Protection Regulation
Analysis of the application network: Privacy and Encryption
1 Authority
8 Advertising Policy
7 Financial Disclosure
Details about the editorial team, and the app team are clearly disclosed.
All adds are identified and clearly separated from the content.
All funding sources and paid services are identified and transparent.

Fig. 27.1 The mHONcode principles dedicated to mobile health apps

Table 27.2 8 principles of the mHONcode regarding the health content of the app

Principles	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 are not ads in the app, does a disclaimer indicate that there is none?

tionnaire with 34 questions related to the mHONcode guidelines. The HON's reviewer analyzes the content of the health app and assesses if it conforms or not to the given principle. For any principles that have not been respected, the HONcode reviewer delivers a detailed report at the end of the process with recommendations on how to improve the health app. This resulting evaluation report helps the health app editor to render content that is HONcode compliant and transparent. The evaluation of health apps for the HONcode takes an average of 180 minutes. Once a health app has been validated, it receives a dated, dynamic, and unique logo it can display on the app store to indicate its annual certification and illustrate the trustworthiness of its construction and maintenance. The seal is located on HON servers, so its status can be monitored and adapted. The HONcode seal is linked to its corresponding HONcode certificate. The latter summarizes the result of the certification of the health app—when and why the health app was certified. When a principle does not respect the recommendations (totally or partially), the health app's editor is requested to do the necessary modifications.

Case Study

The mHONcode in Action

HON chose the ten most downloaded free health apps in the two major stores Google Play and Apple with the limitation of the country in the URL of the stores being France, without discrim-

Table 27.3 Technical consistency, security and privacy of the mHONcode for health apps

Technical consistency, Security and privacy	Type	Implementation request
Detection of weakness and vulnerabilities	Improper Platform Usage	Avoid misuse of a platform feature or failure to use platform security controls.
	Insecure Data Storage:	Avoid insecure data storage and unintended data leakage.
	Insecure communication	Avoid poor handshaking, incorrect Secure Sockets Layer (SSL) versions
	Insecure authentication	Ensure authenticating the end-user when needed or avoid bad session management.
	Insufficient Cryptography	Ensure that cryptography is done correctly
	Insecure Authorization	Avoid any failures in the authorization
	Client Code Quality	Feedback for implementation problems in the app
	Code tampering	Avoid dynamic memory modification
	Extraneous Functionality:	Avoid hidden backdoor functionality
Communication, Privacy & Encryption	Communication security	Application requests/queries must be encrypted with SSL protocol. Authentication (login/password) should be encrypted.
	Data minimization	Only required data must be transferred and used. It prevents excessive bandwidth usage and data leaks.
	Permission minimization	Only required access (camera, location, internet access) must be asked and retrieved with explicit consent.
	Data transfer to third party	Transmission of user data (including IP address) to third party should be done after explicit consent of the user.
Data privacy	Self-Assessment General Data Protection Regulation GDPR (EU 2016/679)	Gathered Data (by the app or a tier) must be done with the explicit consent of the User. Data usage should be compliant with the GDPR. Use HON checklist[a] http://shorturl.at/atITV to identify the improvement necessary to the app services in order to be compliant with the GDPR.

[a] GDPR Self-Assessment HONcode Certification http://shorturl.at/atITV

ination of language, mission, functionalities, and rating. None of these apps had voluntarily required the certification or ever been HONcode certified at the time of the study. As we wanted to test if the GDPR[4] was adopted by apps after this new European regulation came into force across the European Union on May 25, 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 ten 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 ten most downloaded apps between the two stores, on May 24, 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 27.4 and 27.5.

Ten 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 (Tables 27.2 and 27.3) [23]. This new code of conduct also includes two security tests: an automated test for detection of weakness and vulnerabilities and a test about privacy and encryption, which analyzes the application's network, they can be found at the end of Table 27.3. Thus, ten 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

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

Table 27.4 Positions, number of downloads for the ten selected apps on May 24, 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	>one million
Grossesse +	iOS 5.4 Android 5.2	Philips/Health & Parenting	Pregnancy	#2 Medical	#1 Parents	>ten 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
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 Grossesse	iOS 2.6 Android 2.9.0	Doctissimo/TF1/Lagardère	Pregnancy	#10 Medical	#12 Medical	>one million

Table 27.5 Ratings and number of ratings for the ten selected apps on May 24, 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	5800
Qare	4.7/5	567	4.8/5	2000
Staying Alive	4.1/5	2000	4.2/5	2
Sauv Life	3.9/5	786	4.3/5	297
We Moms	4.6/5	9000	4.7/5	129
Mon Ovulation	4.2/5	4000	3.5/5	6
Livi	4.5/5	877	4.9/5	2700
Bébé +	4.5/5	29,000	4.7/5	1300
Ma Grossesse	4.3/5	32,000	4.3/5	34

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[5] allowing to be in between of the app transmission of data over the Internet and the phone. In addition, the Mobile App Security Test,[6] free product by ImmuniWeb, was used to scan the code. For Android, APK or Google play link was used to upload the code, 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 ten apps were downloaded to a HUAWEI P20 Android version 9.0.0, Android 8.1.0 and an iPhone 8 iOS version 12.2.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 eight principles, Table 27.6 shows for each application if it respects each principle. The symbol **X** 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 does not apply to the app. For some principles, we separated the results to be more precise, the signification of each initial is indicated below (Table 27.6).

Summary

As demonstrated in the case study described above, there appears to be no correlation between the popularity of an app and the quality parameters laid out by the mHONcode, which demonstrates that the trustworthiness of the app was not one of the parameters considered by users when choosing it.

It is not surprising, given that mobile apps are still very new. Also, because apps do not provide health information in the traditional sense, like a health website presents pages of health information, it would not be apparent for users to consider trustworthiness as a required characteristic for mobile health apps.

Thus, a way to distinguish trustworthy mobile health apps is required, not only to make them more visible but also to introduce the whole concept of trustworthiness to mobile health app users [24].

As the adaptation of an already proven trustworthy code of conduct of health websites (the HONcode), the mHONcode is well placed to provide guidance for the next generation of health information providers—mobile apps in this case.

Conclusions and Outlook

mHealth is a huge market that 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), they can also process 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 informa-

[5] https://mitmproxy.org/

[6] https://www.immuniweb.com/mobile/#about

Table 27.6 Compliance with each principle for each application—assessment conducted in May 2019

Principles	1. Authority	2. Complementarity	3. Confidentiality		4. Validity (Dates)			5. Justifiability Objectivity		6. User's practice				7. Financial disclosure	8. Advertisement policy	
Apps			Policy	Consent	M	L	A	R	O	M	A	I	S		Policy	Identification
Doctolib	X	NA	X	X	NA	X	X	NA	NA	X	X	X	X	X	X	NA
Grossesse+	X	✓	✓	X	X	✓	X	X	✓	X	✓	✓	✓	X	X	X
Qare	✓	✓	✓	X	X	✓	X	NA	NA	✓	X	✓	✓	X	X	NA
Staying Alive	✓	✓	✓	X	NA	X	X	NA	NA	X	X	✓	✓	✓	✓	NA
Sauv Life	X	NA	✓	X	NA	X	X	NA	NA	✓	✓	X	X	X	X	NA
We Moms	X	✓	✓	✓	X	✓	X	X	✓	✓	✓	✓	X	X	✓	✓
Mon Ovulation	X	X	X	X	X	✓	X	X	✓	X	✓	X	✓	X	X	X
Livi	X	✓	✓	✓	NA	✓	X	NA	NA	✓	✓	✓	✓	X	X	NA
Bébé +	X	✓	✓	X	X	✓	X	X	✓	✓	✓	✓	✓	X	X	X
Ma Grossesse	X	X	X	X	X	✓	X	X	✓	X	✓	X	✓	X	X	X

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

tion, with no need to take an appointment, straight from their pocket, which of course represents massive advancement in healthcare but also a real danger.

As demonstrated by other studies, our study, based on the ten most downloaded mobile apps in France, has shown clearly that mHealth apps, are sharing data that is far from transparent [14, 15]. The non-conformity with the mHealth HONcode guidelines and issues in terms of privacy or security identified could be easily overcome with guidance to the developing team and 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 [25]?

Although, even if only ten apps were used in this study, it should be remembered that the ten 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, as was confirmed with this panel of apps, they represent a real public health danger, which can be overcome only with the commitment of the owners/developers of these apps, which the HON Foundation will try to address through its new code of conduct, the mHONcode.

Review Questions

1. What kind of special risks arise from apps on mobile devices compared to websites?
2. Why is it a problem to assess many features of the app as different frameworks suggest?
3. What are the eight principles of the mHONcode?
4. Please describe the mHONcode certification process!

Appendix: Answers to Review Questions

1. What kind of special risks arise from apps on mobile devices compared to websites?

Websites display the data as they are part of the content of this site which is therefore easy to check also in terms of how they are produced. In apps, the algorithms used to analyze the data are kept secret and are not disclosed because they belong to the business model of the app. The privacy and security of transmission and storage is very difficult to test and assess in apps as well. Apps play the role of a "medical device" even if by definition of the relevant laws they are not which is unlike health websites. They do not play a diagnostic role but only an informational role.

2. Why is it a problem to assess many features of the app as different frameworks suggest?

Too many criteria to be assessed may lead to a situation in which developers are reluctant to have their app assessed due to potentially high costs and inefficient practices. This in turn entails a low number of apps being actually assessed. In contrast, transparency and honesty in the production of the apps will engage developers to disclose what is behind the scene and be responsible to what health app it develops. Furthermore, not all apps need the same attention as they do not imply the same potential risk to consumers. For example, health apps with calculators and algorithms intended to recommend an action or medications may directly impact the user's health and must be scrutinized thoroughly, while diary apps just used for documentation are less critical.

3. What are the eight principles of the mHONcode?

   1. Authority.
   2. Complementarity.
   3. Confidentiality.
   4. Validity.
   5. Justifiability & Objectivity.
   6. User's practice.
   7. Financial disclosure.
   8. Advertisement policy

4. Please describe the mHONcode certification process!

Step 1: The health app owner voluntarily applies via the HON website for the mHONcode certification for manual evaluation by an expert medical team and a security officer according to the mHON principles and associated published guidelines.

Step 2: The health app editor needs to fill in a self-reporting mHONcode questionnaire with 34 questions related to the mHONcode guidelines.

Step 3: The HON's reviewer analyzes the content of the health app and assesses if it conforms or not to the given principle.

Step 4: For any principles that have not been respected, the HONcode reviewer delivers a detailed report at the end of the process with recommendations on how to improve the health app. This resulting evaluation report helps the health app editor to render content that is HONcode compliant and transparent.

Appendix: Definitions of Terms in the Text

Digital engagement: Anything that involves a conversation online.

Digital care: An evidence-based software intervention (a program, application, or the like) that is intended to prevent or treat a disease and carries the attributes below.

Data security: Protective digital privacy measures that are applied to prevent unauthorized access to computers, databases, and websites.

e-Health: e-Health is a broad term, and refers to the use of information and communications technologies in healthcare.

Digital health technology: Digital health, which includes digital care programs, is the convergence of digital technologies with health, healthcare, living, and society to enhance the efficiency of healthcare delivery and make medicine more personalized and precise.

Population health: The health outcomes of a group of individuals, including the distribution of such outcomes within the group.

Encryption: The process of converting information or data into a code, especially to prevent unauthorized access.

Algorithms: A process or set of rules to be followed in calculations or other problem-solving operations, especially by a computer.

Cryptography: A method of protecting information and communications through the use of codes, so that only those for whom the information is intended can read and process it.

Data minimization: The principle of data minimization involves limiting data collection to only what is required to fulfill a specific purpose.

References

1. IQVIA Institute for Human Data Science. 2017 The growing value of digital health evidence and impact on human health and the healthcare system. https://www.iqvia.com/insights/the-iqvia-institute/reports/the-growing-value-of-digital-health [Accessed July 2020].
2. Research 2 Guidance. mHealth App Economics 2017/2018 Current Status and Future Trends in Mobile Health Research2Guidance report. USA, 2017, pp 10. https://research2guidance.com/product/mhealth-economics-2017-current-status-and-future-trends-in-mobile-health/ [Accessed May 2019].
3. Business Insider. *10 Ways Mobile Is Transforming Health Care* https://www.businessinsider.fr/us/10-ways-mobile-is-transforming-health-care-2014-6 [Accessed August 2020].
4. Zhang C, Zhang X, Halstead-Nussloch R. Assessment metrics, challenges and strategies for mobile health apps. Issues Inform Syst. 2014;15(2).
5. Day S, Zweig M. Rock health beyond wellness for the healthy: digital health consumer adoption 2018, 2019. https://rockhealth.com/reports/beyond-wellness-for-the-healthy-digital-health-consumer-adoption-2018/
6. Martínez-Pérez B, De La Torre-Díez I, López-Coronado M. Privacy and security in mobile health apps: a review and recommendations. J Med Syst. 2015;39(1):181.
7. Schechner S, Secada M. Feb 2019 You Give Apps Sensitive Personal Information. Then They Tell Facebook. Wall Street J. https://www.wsj.com/articles/you-give-apps-sensitive-personal-information-

then-they-tell-facebook-11550851636 [Accessed August 2020].

8. McKay FH, et al. Evaluating mobile phone applications for health behaviour change: a systematic review. J Telemed Telecare. 2018;24(1):22–30.
9. Carroll JK, et al. Who uses mobile phone health apps and does use matter? A secondary data analytics approach. J Med Internet Res. 2017;19(4):e125.
10. Huckvale K, et al. Unaddressed privacy risks in accredited health and wellness apps: a cross-sectional systematic assessment. BMC Med. 2015a;13:214.
11. Huckvale K, Adomaviciute S, et al. Smartphone apps for calculating insulin dose: a systematic assessment. BMC Med. 2015b;13(1):106.
12. Plante TB, Urrea B, et al. Validation of the instant blood pressure smartphone app. JAMA Intern Med. 2016;176(5):700–2.
13. Wisniewski H, Liu G, Henson P, Vaidyam A, Hajratalli NK, Onnela JP, Torous J. Understanding the quality, effectiveness and attributes of top-rated smartphone health apps. Evid Based Ment Health. 2019;22(1):4–9.
14. Grundy Q, Chiu K, Held F, Continella A, Bero L, Holz R. Data sharing practices of medicines related apps and the mobile ecosystem: traffic, content, and network analysis. BMJ. 2019;364:l920.
15. Huckvale K, Torous J, Larsen ME. Assessment of the data sharing and privacy practices of smartphone apps for depression and smoking cessation. JAMA Netw Open. 2019;2(4):–e192542.
16. DG CONNECT. https://ec.europa.eu/digital-single-market/en/mhealth [Accessed August 2020].
17. Food and Drug Administration (FDA). 2017 Mobile medical applications: guidance for industry and food and drug administration staff. URL: goo.gl/oZGjNE [Accessed August 2020].
18. European Commission. Code of Conduct on privacy for mobile health applications. URL:goo.gl/mFbK47. https://ec.europa.eu/digital-single-market/en/news/code-conduct-privacy-mhealth-apps-has-been-finalised [Accessed August 2020].
19. Levine DM, Co Z, Newmark LP, et al. Design and testing of a mobile health application rating tool. npj Digit Med. 2020;3:74. https://doi.org/10.1038/s41746-020-0268-9.
20. The United States Department of Commerce. Code of Conduct for mobile application (“app”) short notices on Application Transparency, 2013. Accessed: 2017-11-14. URL: https://goo.gl/eAKKcf
21. Kumar N, Khunger M, Gupta A, Garg N. A content analysis of smartphone-based applications for hypertension management. J Am Soc Hypertens JASH. 2015;9:130–6.
22. Boyer C, Gaudinat A, Hanbury A, Appel RD, Ball MJ, Geissbühler A, et al. Accessing reliable health information on the web: a review of the HON approach. Stud Health Technol Inform. 2017;245:1004–8. https://doi.org/10.3233/978-1-61499-830-3-1004.
23. Ranasinghe M, Cabrera A, Postel-Vinay N, Boyer C. Transparency and quality of health apps: the HON approach. Stud Health Technol Inform. 2018;247:656–60.
24. Postel-Vinay N, Jouhaud P, Bobrie G, Boyer C. Home blood pressure measurement and mobile health app for pregnant and postpartum. J Hypertens. 2019;37:e280. https://doi.org/10.1097/01.hjh.0000573576.89014.cb.
25. Research 2 Guidance 2018 mHealth Economics – How mHealth App Publishers Are Monetizing Their Apps https://research2guidance.com/product/mhealth-economics-how-mhealth-app-publishers-are-monetizing-their-apps/