JMTM
WWW.JOURNALMTM.COM

ORIGINAL ARTICLE

Evaluation of Free Android Healthcare Apps Listed in appsanitarie.it Database: Technical Analysis, Survey Results and Suggestions for Developers

Dr. Lorenzo Di **Matteo**[1], Dr. Carmela **Pierri**[2], M.D. Sergio **Pillon**[3], Eng. Giampiero **Gasperini**[4], Eng. Paolo **Preite**[1], Dr. Edoardo **Limone**[4], Dr. Silvia **Rongoni**[1]

[1]Department of Training, Formit Foundation; [2]Board of Directors, UNINT University/ Department of Training, Formit Foundation; [3]Department of Cardiovascular Telemedicine, Azienda Ospedaliera San Camillo-Forlanini; [4]Department of Strategy and Technologies, Formit Foundation

Corresponding Author: l.dimatteo@formit.org

Background: Health apps catalogued in dedicated databases are not scarce but still little is known about the situation concerning their technical aspects such as the general level of privacy and security.

Aims: This study aims to analyze android free health apps in a specific database.

Methods: A systematic technical analysis on a population of 275 android free app among the ones listed in the *appsanitarie.it* database ("*Banca Dati delle app sanitarie*"). Analysis has been carried out following a defined protocol with a survey as operative support tool to examine aspects such as the app rating in the store.

Results: The analysis concerned 275 health apps. Cardiology (38 apps) resulted to be the most populous medical branch. The overall app ratings average is 4,10. 18,54% of the apps required personal data at first launch. 84,36% of the apps allowed only manual data entry. Data sharing has been detected in 133 cases. 9,45% of the apps provides a backup option. 13% of the apps declare to be compliant to some kind of privacy regulation. Among this 13% of apps only 19% showed relevance to the EU privacy regulation. The 61,1% of the apps presented no reference for scientific background of the contents.

Conclusions: Manual data entry when redundant should be avoided by developers in favour of automatic calculation of derived parameters. Moreover a limited number of the analyzed apps adopt data protection mechanisms and declare privacy compliance. Security and Privacy are generally poor. Survey results suggest there is large room for improvement in app design.

Keywords: Telemedicine, eHealth, mHealth, Data Security, Baseline Survey

Journal MTM 7:2:17–26, 2018 doi:10.7309/jmtm.7.2.3 www.journalmtm.com

Introduction

Apps on mobile devices such as smartphone offer a lot of perspectives of use in health and medical fields. App economy as the whole range of economic activity related to mobile applications evolve rapidly as the smartphone market. Other studies report that only the first 10 top mobile health apps generate up to 4 million free and 300.000 paid downloads per day[1].

On the other side Healthcare researches find that vast majority of professionals is conscious of an interoperability lack for a better use of patient generated data[2]. Other researches show that more than half of the interviewed patients assert to have used a digital device including mobile apps to manage their health and almost two thirds think it would be helpful for their healthcare providers to have access to their patient generated data as part of their medical history[3].

Studies showed that for patients with chronic diseases it is a comfortable solution sharing data with healthcare providers via online patient portal, mobile apps or message texts[4]. This could lead to some sort of benefits for both patients and healthcare providers but also expose to some risks, especially the first ones[5,6]. Unclear disclosures about data processing terms could lead to privacy risks for the user and insufficient security could bring to data breaches or loss risks, considering also that a smartphone loss could bring to a leakage[7]. Security or data protection could be not sufficient if the user is not fully capable to prevent the loss of data from the device or mechanisms as encryption or passwords are not available[8].

On the other hand sharing patients health data with messaging and multimedia mobile applications as communication channels it's handy for a professional but non completely compliant with health data protection standards a healthcare trust certainly adopt[9]. On the patient side new findings concluded that while less than half of the analyzed apps are useful to the targeted user, some apps seemed to sacrifice quality and safety to add more functionalities[10].

The purpose of this study is to make a technical analysis of free android apps listed in a dedicated "healthcare apps" database, "*Banca Dati delle app sanitarie*" (at http://www.appsanitarie.it/banca-dati-app-sanitarie). The database has been developed as part of a Formit Foundation project financed by a grant of the General Directorate of Medical Devices and Pharmaceutical Service of the Italian Ministry of Health in 2015-2016. Launched in 2015 the database was created to list results of the apps census operated by the Observatory of the health apps established by Formit Foundation.

Apps in the database has been selected through a specific definition, "healthcare apps", and selection workflow (see methods section for a full description). Database apps, both Android and iOS, have been selected through specific criteria in the stores (summoned in a workflow), and could be used in an healthcare context by patients and physicians. The database apps considered are 659 "healthcare apps", divided in medical branches and 2% of them present a CE mark as medical device. The database has been chosen as starting point for the selection of listed apps because of a clear definition and a selection workflow.

The study which results will be here presented has not been conducted looking in the inner working mechanisms of the apps but with a highly technical analysis of the functionalities available to users. Analysis has been carried out facing four different groups of app characteristic: the app general details; the features as requested data, data entry, data access, connect-ability, online and sharing feature; password and backup security mechanisms; privacy terms and scientific references. Regulatory framework considered in matter of privacy is the *General Data Protection Regulation*, GDPR (Regulation EU 2016/679)[11] due to its validity all over national member states legislations, and the Privacy Code of Conduct on mHealth apps for what concerns guidelines to enhance privacy in this field[12].

Methods

Ethical statement

This research project has been conducted with full compliance of research ethics norms. Research involved usage of mobile devices and apps. Survey development and data gathering involved part of the research team while survey fulfillment another one. Results analysis has been carried out by the whole team.

App selection

Apps has been selected among the list of free Android ones (Google play downloadable) in every medical branch composing the database (*Banca Dati App sanitarie*, BDA http://www.appsanitarie.it/

banca-dati-app-sanitarie). It was also decided to exclude from the analysis apps requiring registration with medical credentials to dedicated platform or specific devices to work. Apps listed in the database has been chosen before this study following a specific definition and a workflow. In this sense not all the health apps could be listed in the database.

Apps defined as healthcare apps (*App sanitarie*) in the database are:

- CE marked Medical device apps (in order to achieve CE mark for their products in Europe, medical device manufacturers must comply with the appropriate medical device directive set forth by the EU Commission);
- Apps not developed with medical purpose by the producer but responding to one of this characteristics:
  - receive data from medical devices;
  - elaboration and transformation of healthcare and patient-related data;
  - interaction with a non medical device that visualize, memorize, analyze and transmit data;
  - receive health data by user with manual entry that are not only diet and fitness oriented.

According to the app definition this workflow was used:

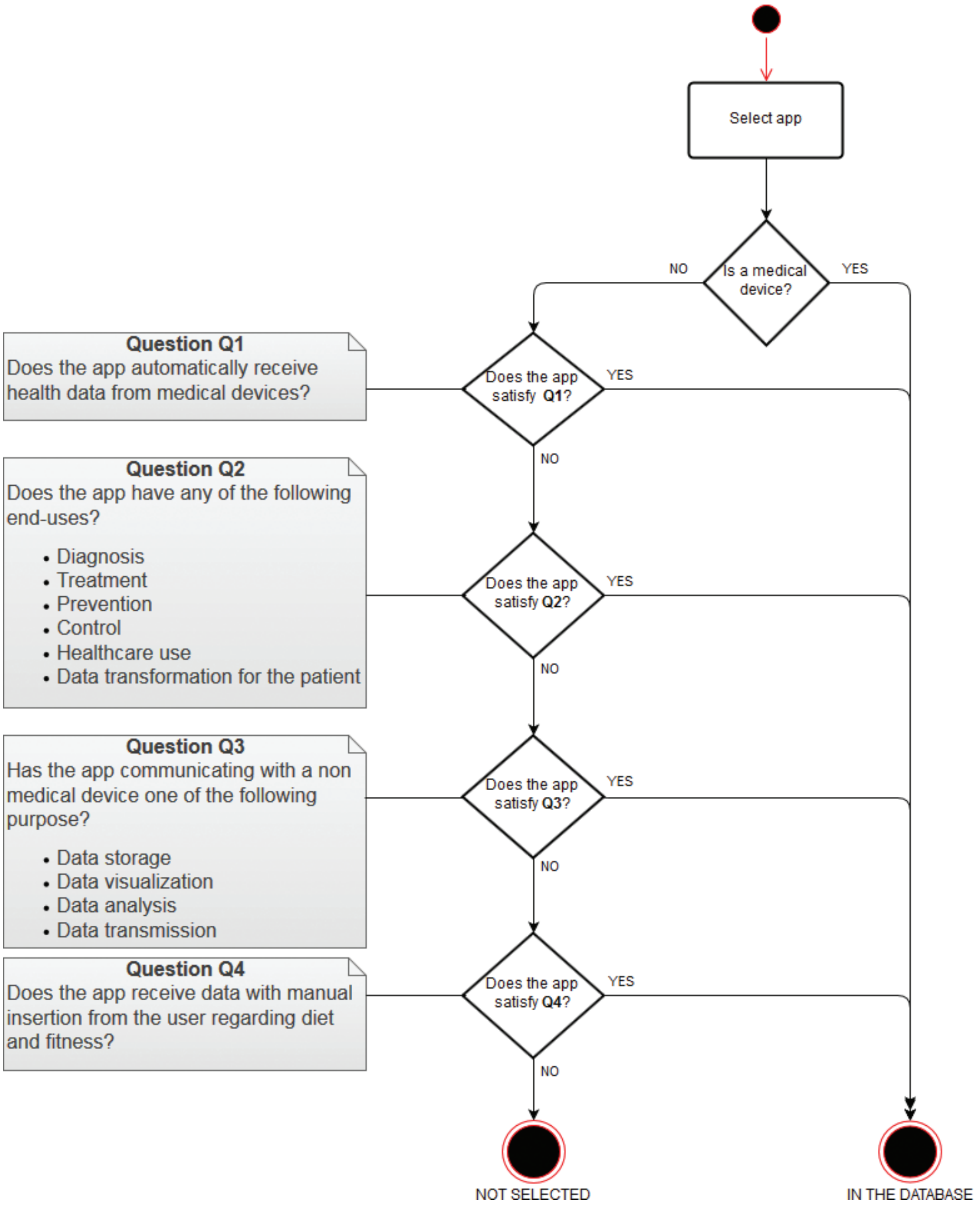

Figure 1: App Selection Criteria

The apps selected from the database to be analyzed satisfy the following operative criteria:

- Available for Android (downloadable from Google play);
- Free;
- With no mandatory registration to platform requiring medical credentials;
- Usable independently from connection with external devices.

Technical analysis

Apps have been under a phase of technical analysis for 2 months, from March to April 2017.

The scope of the technical analysis is to examine some of the operating mechanisms of the selected apps. This has been done following a *Technical Analysis Scheme* characterized by different technical macro-area to identify diverse functional aspects and a metrical-statistical question-answer structure to ensure results measurability and repeatability.

To reach a technical analysis of the software, a survey has been designed and fulfilled. The analysis has been conceived to focus on the following elements:

- Information useful to identify the app;
- Operating characteristics of the app;
- Security related to password, back-up and data encryption;
- Presence of privacy and condition terms.

The technical analysis has been composed by the survey development, comprehensive of design and deployment, and a consequent phase of app analysis, then data gathering and results analysis.

Survey development

To analyze selected apps a survey has been designed with different sections related to different type of data to collect about the four analytics aspects and organized following an answer-question structure. In this sense the sections which composed the survey are:

- *App general characteristics*, as name, version, developer name, rating on the store;
- *App features*, as requested personal data, modality of data entry, possibility to delete/change data, connect-ability, online platform registration, sharing on social media;
- *App security*, as password registration, password recovery, password security level, back-up possibility, backup destination, backup encryption;
- *App privacy and reliability*, as declaration of compliance to some privacy regulation, European privacy regulation compliance, scientific source or bibliography.

The online survey has been realized with the open source application Lime Survey.

App analysis

Technical-functional analysis has been performed accessing the survey through authentication via username and password. Mobile devices with Android operative system have been used with the newest version of operative system available at the time. App search has been performed on the Google Play store. Download has followed if for free and if available in the country where the study took place (Italy). Once installation terminated, mandatory healthcare professional-only platform registration and necessary external device connection has been checked. If negative, the app has been analyzed through the survey fulfillment.

Data gathering and Results analysis

Through Lime survey data gathering has furnished the overall amount of data from the technical analysis. Results analysis instead has been realized on a compiled single dataset, using descriptive statistics to summarize and underline aspects of data collection. Collected data analysis has been accomplished through the data stored in a database managed directly by the application Lime survey, this allowed to export information in formats suitable for statistical work purposes.

Results

App general characteristics

The analysis concerned 275 apps on the total amount of 659 in the database at the time the study took place, due to the existence of operative criteria described in the methods section. Most populous medical branch resulted cardiology (38 apps), oncology (22) and health & well-being (21), as shown in Figure 2.

App rating in the store is expressed on a Likert scale from 1 to 5 by the user and shows the average of the overall amount of rating for an app on an incremental scale. Rating average of an app has been rounded down due to simplify data collection management. The average of the overall app rating averages resulted 4,10, where the lowest app rating average is

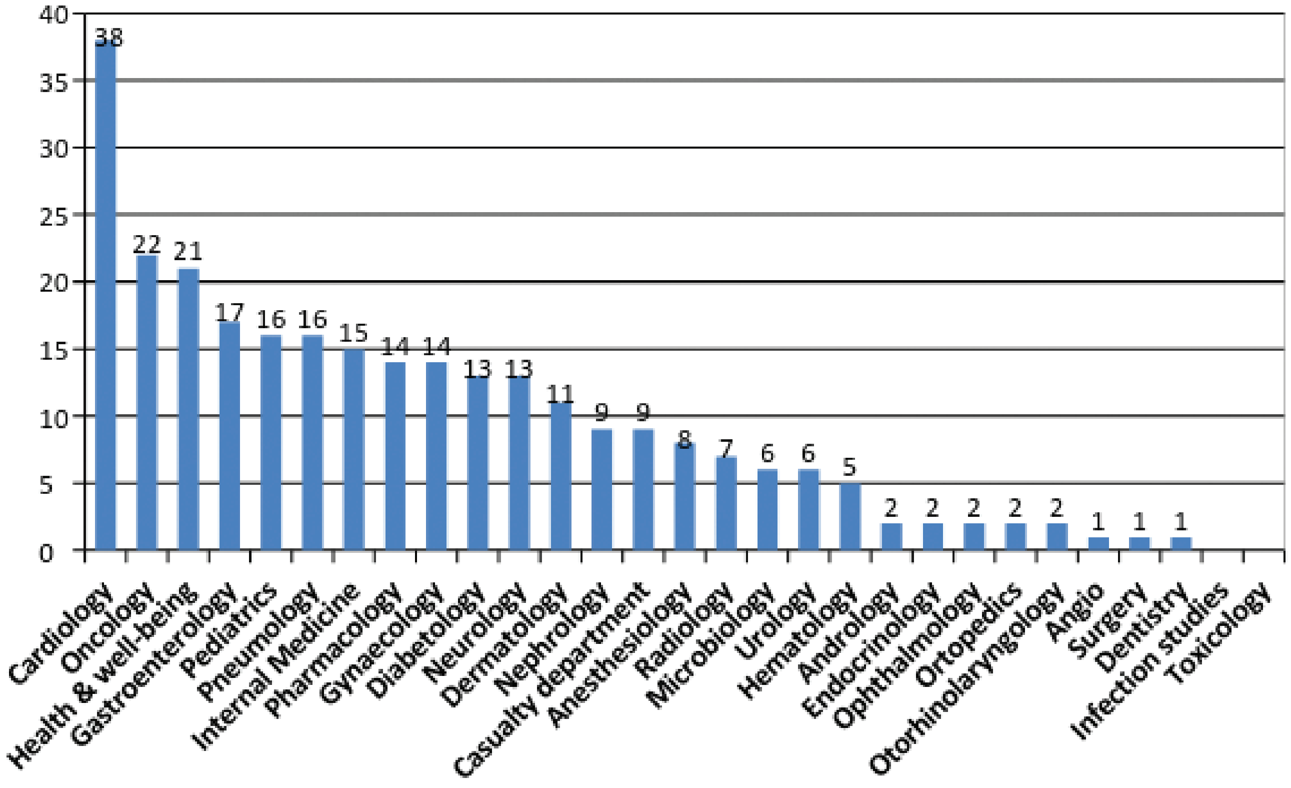

Figure 2: Number of apps per medical branch

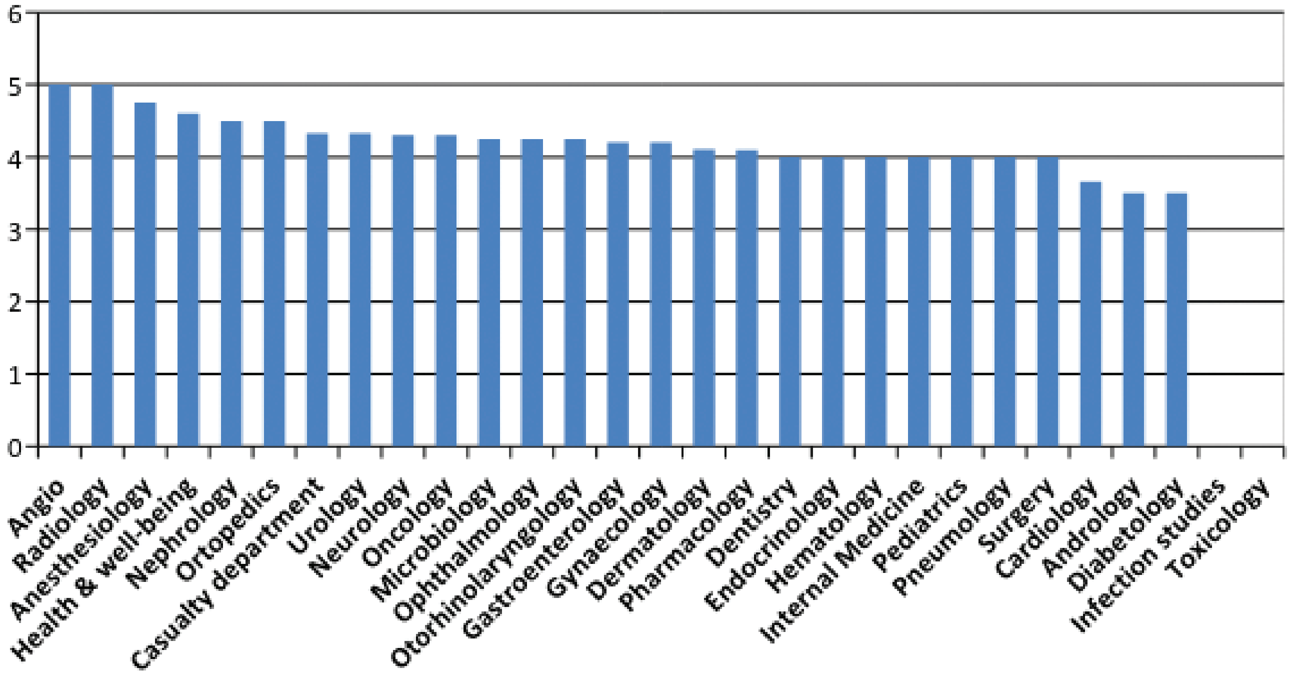

Figure 3: Average app rating per medical branch

1 and the higher is 5. In the most populous medical branches, average of the app rating averages in cardiology is 3,66, while in oncology is 4,33 and in health & well-being is 4,60.

As Figure 3 shows average app rating in the store is high almost for every medical branch in line with the data of an average of the app rating averages of 4,10 on the Likert scale. In fact most of the analyzed

Rating Average	Number of apps	% on the total amount
5	34	12,60%
4,5	91	33,70%
4	105	38,89%
3,5	23	8,52%
3	13	4,81%
2,5	2	0,74%
2	0	//
1,5	0	//
1	2	0,74%

Table 1: Rating average per number of apps

Personal Data required to the user	Number of apps requiring	% on the total amount
At the launch	51	18,54%
Name	15	5,45%
Surname	11	4%
Date of birth	20	7,27%
Gender	41	14,91%
Age	32	11,62%
Weight	24	8,62%
Height	14	5,10
Blood type	0	0

Table 2: Personal Data required at first launch per number of apps

apps resulted to be placed in the high ranks of the rating scale. Excluding 5 apps with no rating on the store, 105 on 270 apps, the 38,89% of the overall rated apps resulted having a rating average of 4 while 91 apps, the 33,70% is ranked with an average of 4,5 and 34 apps, the 12,60% showed a rating average of 5. However rating in the store could be subjected to distortive mechanisms such as comments directly or indirectly linked to the developers or an exiguous amount of them.

App features

Generally health-ish apps need data input to perform one or more of their features. In this sense 18,54% of the analyzed apps showed to require personal data at their first launch in order to create a user profile. An app can request to the user one or more of the data listed in Table 2. The most frequently required data resulted to be gender for the 14,91% of the apps (41), followed by age the 11,62% (32) and weight the 8,62% (24).

Modality of data entry followed the part of the survey section concerning personal data request. Data entry could happen through a possible synchronization with an external device in order to acquire data automatically, or at the contrary only manually or both. The great majority of the apps allowed only manual data entry, exactly 84,36% (232) of the apps. Only automatic and both data entry modality are allowed by the 8% and the 7,64% of the apps.

Similarly results about possibility to change and delete entered data showed that it was possible manual change for the 84% of the apps and manual deletion for the 72,72%. It has been noticed that it was not possible change manual entered data only for 18 apps and no possibility to delete for 47. Only 5,45% of the analyzed apps resulted to allow the modification of automatic entered data and 6,18% the deletion. In this sense results of N/A change and delete of automatic entered data and the possibility to

Modality of data entry	Number of apps	% on the total amount
Only automatic	22	8%
Only manual	232	84,36%
Both automatic and manual	21	7,64%

Table 3: Modality of data entry per number of apps

Possibility to change and delete data	N/A	YES	NO	YES % on the total amount
Change automatic entered data	247	15	13	5,45%
Delete automatic entered data	248	17	10	6,18%
Change manual entered data	26	231	18	84%
Delete manual entered data	28	200	47	72,72%

Table 4: Communication protocols per number of apps

Communication Protocols	Number of apps	% on the total amount
Bluetooth	14	5,1%
Wi-Fi	15	5,45%
USB	1	0,36%
Dedicated interface	1	0,36%

Table 5: Communication protocols per number of apps

change and delete manual entered data or vice versa almost match.

In line with the previous survey results, regarding communication protocols to exchange data with other systems or external medical devices, the most used resulted Wi-Fi for the 5,45% of the apps, followed by Bluetooth for the 5,1%. USB and a dedicated interface resulted to be used as communication protocols only by two of the analyzed apps.

In relation to communication and data exchange with online data storage services it was analyzed diffusion of mandatory registration to online platform in order to completely use the app. Generally apps requiring registration to an online platform permit backup of the data composing the user profile through a dedicated feature. In this sense it turned out to be only a 3,63% of the apps to require a mandatory registration to an online platform.

A considerable number of analyzed apps presented the feature "share" on different communication channels and social media. An app can allow more than one data sharing possibility. On the overall 133 times data sharing has been detected, the most frequent data sharing feature resulted to be e-mail (45 apps), almost doubling the second one that is SMS (23). Sharing on social media resulted to be possible only with 17 apps on Facebook and 14 on Twitter. Other channels not considered initially in the survey but of which it has been taken note in dedicated blank spaces, were hangouts resulting 12 times as social media and 10 times google drive as other sharing channel.

Mandatory registration to an online platform	YES	NO	% on the total amount
Obligation to register	10	265	3,63%

Table 6: Mandatory registration to online platforms per number of apps

App security

Results regarding app security and data protection showed that only few of the analyzed apps provides password registration. The 5,1% of the apps shown to provide the creation of a password at the app start and only the 1.1% a secured password. On the overall amount of apps only 1,81% provides the password recovery generally known as "Forget Password?" button sending the new password to a previously saved email address.

For what concerns data storage option it resulted to be possible both locally, on the smartphone memory, that remotely with online storage services. Globally 9,45% of the overall analyzed apps provides a backup option. An online backup has been possible for the 5,1% of the apps, while a local memory back-up for the 4,36%. Regarding a clear-to-the-user encryption of the backup, 5,81%

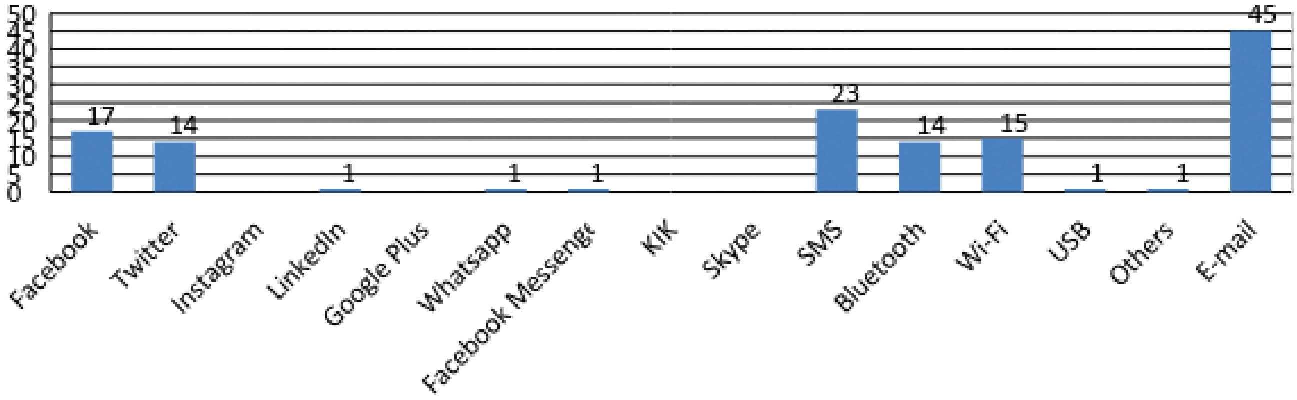

Figure 4: Data sharing channels per number of apps

App security and data protection	Number of apps	% on the total amount
Password at application start	14	5,1%
Secured password	3	1,1%
"Forget Password?" feature	5	1,81%
Back-up option	26	9,45%
Local Memory Back-up	12	4,36%
Online Back-up	14	5,1%
No Viewable Back-up Encryption	16	5,81%

Table 7: App security and data protection

of the overall apps, more or less the all apps with backup option, showed no possibility to have clear information about encryption. Naturally it has been not feasible to check for encryption for the vast majority of the apps (93,81%) having no back-up.

App privacy and reliability

App analysis concerning privacy showed that only 13% of the all apps declare to be compliant to any kind of privacy regulation for what concerns personal and health data about the user. The 87% of the apps showed no declaration of compliance to any kind of privacy regulation with any kind of message to the user, nor at launch nor in the menu.

Among this 13% of apps showing a declaration of privacy regulation compliance only 19% showed some sort of relevance to the EU privacy regulation. This is due to the fact that national regulation of Member States has been considered in relation to a wider European privacy regulation. In fact before *General Data Protection Regulation*, Directive 95/46/CE has been adopted by data protection and privacy national acts. The 81% of the remaining apps showed instead an international declaration related to an End-User License Agreement (EULA) model or some other type of generic declaration. For what concerns reliability it has been considered the presence of references quoted in the app regarding scientific sources. Generally scientific references and quotes has been found in the info or in the bibliography section of the app menu. The 61,1% of the analyzed apps presented no reference or quote regarding the scientific background of the contents, while 38,18% presented a bibliography or quoted studies in a dedicated part of the menu and 1,81% resulted to be not applicable to this check.

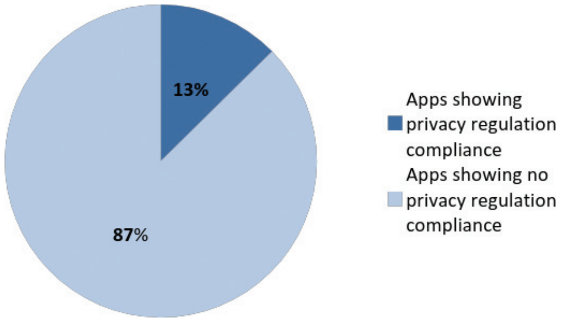

Figure 5: Percentage of Apps Showing Declaration of Privacy Regulation Compliance

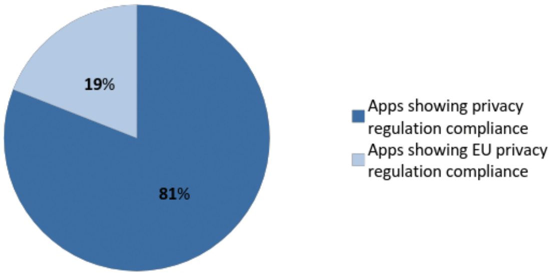

Figure 6: Percentage of apps showing EU privacy regulation Compliance among apps declaring privacy regulation compliance

Reliability based on scientifical references	% of NO	% of YES	% of N/A
Presence in the app of references and quotes	61,10%	38,18%	1,81%

Table 8: Scientific references in the app

Discussion

It is expected that Bring-Your-Own-Device connectivity will be preferred by select patient groups and will be used for the remote monitoring of 22.9 million patients in 2021[13]. In this sense it is no surprise the number of health apps in the stores like Google Play, although the number of apps wears thin using a database based on a specific definition of mHealth app with a clearly defined selection workflow. Another boundary for the analysis has been represented by the possibility of free download and analyze functionalities without restrictions of use by necessary external device to operate or mandatory registration to platform requiring medical credentials.

On the other hand the strict database selection criteria and subsequently the limits of analysis operative criteria have brought to a homogeneity of apps population and uniformity of characteristics to analyze. Concerning the definition of app on which the database is based certainly the app analysis selection has been made among a population of apps that excludes low quality apps from the analysis spectrum. In this sense it has to be explained the small numbers of analyzed apps for some specialized medical branches and limits of findings for apps in those branches.

Likert scale is an important score to observe regarding adoption of an app by users. Although this data could be subjected to some distortions and elaboration of new assessing tools doesn't miss[14-18]. Usability is generally measured with the perceived ease and enjoyment experiencing in using the app[19], but the user could rate poorly an application with solid data security mechanisms but no catchy layout and the opposite with a more attractive but less secure app. Therefore rating of the apps is certainly important albeit partial.

The request of personal data opens up other considerations. Processing personal data would suggest the adoption of a database encryption mechanism, but once "compiled" in the form of "application package" can no longer be opened and verified without violating the copyright of the developer. It is also true that both Apple and Google have enabled encryption of the application database in the default mode.

It should also be noted that requiring to the user both age and date of birth impacts on data quality management. Most of the apps allow only manual data entry. It is an important factor due to its possible repercussion on data quality. Essentially more it is reduced input error, more data quality will be achieved. However data entry could be manual due to a developer lack or to a functional condition to respect in order to let the app run.

Regarding automatic data entry some applications use communication protocols with other systems or external devices as Bluetooth, wi-fi or USB. Regarding data exchange, Android allows the developer to easily implement communication to social networks or instant messaging systems with the possibility of data sharing with other users. Mail choice to share data is no surprise, the versatility of the medium is certainly more suitable to send ordinary messages to a doctor. Similarly SMSs are used by apps to share data since many applications elaborate a set of numeric values that can be easily included into a text message.

In matter of data protection the use of a secure password with a minimum of eight letters and alpha-numeric symbols seems to be rare. In this sense a personal identification number of five digits can be easily forced by a brute force attack trying all the possible combinations. It's worth to mention also that a strong password is a condition that could be set up by design.

The apps including a backup function resulted to be limited too, but when the app not requires "persistent" data to trace, backup is useless. More than half of the analyzed apps has backup on online services (a cost to the app provider that local memory backup isn't). The user could be not adequately aware of the technical and legal mechanisms that regulate the cloud computing service[20], local backup instead allows complete data management. No sufficient information about data protection controls has been noticed. This is because the focus in the app description on the store generally seems on advertising, while neglecting privacy and security reliability.

The great majority of the apps showed no declaration of compliance to any kind of privacy regulation. Calculator apps or similar apps resets at every exit deleting all the entered data with no real data processing. Anyway it doesn't really explain the absence of scientific references and quotes in almost 6 on 10 apps. In fact only a few apps presented clear scientific references. For some apps, especially scale calculator a professional may not need scientific references to identify or use a well-known tool in his or her medical branch, but for a user with no particular knowledge in medical science the lack of information could lead to misreading the outcome and to false negative self-diagnosis.

Conclusions

Considering that the analysis has been carried out on a limited number of apps, data-quality oriented approach should be used anyway by developers in order to realize a correct balance between manual data entry and automatic calculation. Manual data-entry should be reduced and the automation should be increased. Moreover format-control parameters or different controls (as sliders, or date-picker) should be used to reduce data-entry mistakes. Replacement of the classic text-field produces an increasing of speed during the filling process and reduces typing errors. In this sense could be useful to look for a better understanding of the perceived and desired usability by the user, rising research attention on this side. On the other hand it is necessary to examine feasibility of mHealth in the healthcare context, as effectiveness of mobile phone applications in healthcare services. In this sense a pathway could be an observational studies by experimenters with patient or physicians adopting mHealth solutions.

Acknowledgements

We would like to thank the General Directorate for Medical Devices and the Pharmaceutical Service of the Ministry of Health (Italy), especially Dir. Marcella Marletta, Eng. Pietro Calamea and Dr. Paola D'Alessandro for their support.

References

1. Mobile Health Market Report 2013-2017, research2guidance, March 2013:7.
2. Compton-Phillips A, What Data Can Really Do for Health Care, Care Redesign, Nejm Catalyst, March 2017:6-7.
3. Patient Expectations of Medical Information Sharing & Personalized Healthcare, Trascend Insights, Survey Report, February 2017.
4. The 2017 Patient Engagement Perspectives Study, CDW Healthcare, 2017.
5. Mitigate Cyberattacks with HIPAA-Compliant Communications, HIPAA White Paper, 2017.
6. Mobile Malware Evolution 2016, Kaspersky Lab, March 2016.
7. "*What A Difference A Year Makes*", Healthcare Breach Report, Bitglass, January 2016.
8. *"Is Your Data Security Due For a Physical?",* Healthcare Breach Report, Bitglass, January 2015.
9. DeepMind Health Indipendent Review Panel Annual Report, July 2017:14.
10. K. Singh, K. Drouin, L. P. Newmark et al., Developing a Framework for Evaluating the Patient Engagement, Quality, and Safety of Mobile Health Applications, The Commonwealth Fund, February 2016.
11. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (referred also as General Data Protection Regulation) http://eur-lex.europa.eu/legal-content/GA/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG.
12. Privacy Code of Conduct on mHealth apps, https://ec.europa.eu/digital-single-market/en/privacy-code-conduct-mobile-health-apps.
13. mHealth and Home Monitoring – 8th Edition, Berg Insight, February 2017.
14. Stoyanov, Stoyan R et al. "Mobile App Rating Scale: A New Tool for Assessing the Quality of Health Mobile Apps." Ed. Gunther Eysenbach. JMIR mHealth and uHealth 3.1 (2015): e27. PMC. Web, 26 July 2017.
15. Stoyanov, Stoyan R et al. "Development and Validation of the User Version of the Mobile Application Rating Scale (uMARS)." Ed. Gunther Eysenbach. JMIR mHealth and uHealth 4.2 (2016): e72. PMC. Web. 27 July 2017.
16. Domnich, Alexander et al. "Development and Validation of the Italian Version of the Mobile Application Rating Scale and Its Generalisability to Apps Targeting Primary Prevention." BMC Medical Informatics and Decision Making 16 (2016): 83. PMC. Web. 27 July 2017.
17. Bradway, Meghan et al. "mHealth Assessment: Conceptualization of a Global Framework." Ed. Mircea Focsa. JMIR mHealth and uHealth 5.5 (2017): e60. PMC. Web. 27 July 2017.
18. Baptista, Shaira, Brian Oldenburg, and Adrienne O'Neil. "Response to 'Development and Validation of the User Version of the Mobile Application Rating Scale (uMARS).'" Ed. Gunther Eysenbach. JMIR mHealth and uHealth 5.6 (2017): e16. PMC. Web. 27 July 2017.
19. J. Nielsen, Usability 101: Introduction to Usability, January 4, 2012, https://www.nngroup.com/articles/usability-101-introduction-to-usability/.
20. Griebel, Lena et al. "A Scoping Review of Cloud Computing in Healthcare." BMC Medical Informatics and Decision Making 15 (2015): 17. PMC. Web. 27 July 2017: 13.