Imperial Journal of Interdisciplinary Research (IJIR)
Vol-3, Issue-9, 2017
ISSN: 2454-1362, http://www.onlinejournal.in

Assessing and Fostering Responsible Practice in Mobile Application Development

APURU J. I.[1], AUDU K. D.[2] & ANDEMBUBTOB D. R.[3]
[1, 2, 3] Department of Mathematical Sciences, Taraba State University, Jalingo

Abstract*: As mobile devices such as Smartphones and other handheld, Personal Digital Assistants (PDAs) continue to permeate human life today, each sector of society is seeking to partake in the benefits thereof. The Health sector is not left behind as today there is a large number of mobile devices and applications that are used in health areas such as in checking vital signs, in diagnosis, suggesting healthy diets, etc. Knowledge of the level of adoption of responsible practices in Mobile Applications Development remains limited. We therefore propose a research on the investigation of, and intervention with the current state of applying responsible practices in mobile application development to bridge the knowledge gap. Our study shows that most developers of Mobile Health Applications (mHealth apps) do not take into serious consideration responsible practices during the development of their apps. While some developers are ignorant of Responsible Research and Innovation, others are somewhat negligent to adopt responsible research because of non-incentives or non-punishment of defaulters.*

1. Introduction

The use of mobile devices, especially smartphones, continues to revolutionize human life and every sector of society seeks to benefit therefrom. The Health sector is also actively involved in this revolution today, resulting in the use of so many mobile devices and applications in health areas such as in vital signs monitoring, minor diagnosis and suggesting health diets and so on. The increase in availability of these smart devices causes a general increase in the integration of computing technologies into our professional, social and private lives. The ubiquity of computing comes with enough ethical issues and concerns that needed to be known by both computer professionals and users. We propose a research on the investigation of, and intervention with the current state of applying responsible practices in mobile applications development particularly focusing on requesting, collecting, storing and processing user personal data such as identity, location, network usage, etc. especially in the health sector. We argue that the development of mobile applications should follow the principles of *Responsible Research and Innovation* (RRI) as it deals greatly with users' personal and privacy data. Responsible Research and Innovation in mobile applications can boost user confidence in the use of mobile applications, and therefore increase their popularity.

This research aims to find out whether developers of mobile applications (particularly those of mHealth apps) apply responsible practices in collecting and using personal data from users; and to discover what could be done to make them more readily adopt responsible practices when they collect, use and manage users' private data. A number of Mobile Health Applications (mHealth apps) are analysed to identify the private data they require from users; and to classify evidence where excessive and unnecessary access to user privacy is attempted; focusing on the permissions requested by these mobile apps. We analyse patterns in terms of responsible practices of data collection by the apps and show how third-party components could also affect the resulting product (Mobile Apps); for example, "…potential privacy and security risks [also] posed by embedded or in-app advertisement libraries" as stated by [4].

We present the results of our findings and recommendations on how to make mHealth apps developers improve upon responsible practices which will better protect the privacy of their users' personal data.

2. Best Practices in mHealth Apps Development

Best Practice could be seen as an approach or a method which is generally accepted over other alternatives due to superior results it produces or achieves; or maybe because the method has become a normal way in which things are done; like a normal way ethical and/ or legal requirements are complied with; as seen by [13]. In other words, we can refer to Best Practice as Professional or Commercial procedure or method which is generally accepted as right. Best Practice is determined through experience and study and is proven to be reliable and to produce the desired result.

2.1. Ethics in mHealth Apps Development

Developers of mHealth apps need to consider the necessary Ethics while developing mHealth apps. Ethics describes a system of moral principles affecting the way individuals and groups of people live and run their lives and how they make decisions. It concerns what individuals, cultures or organizations see as right. [7] views computer ethics as the nature and social impact of computer technology together with the corresponding policies formulation and justification for regulating the use of such technology. In computing; for example, Ethics is observed by both professionals and users of computing devices; [1]. The moral principles that make up Ethics include those spelling out what a member's rights and/ or responsibilities are; what makes something good/ right or bad/ wrong; and so on. Stakeholders' rights need to be protected while they also take responsibilities in observing and respecting others' rights and also their own collective rights.

3. Problem Formulation

Central to this study are the following research questions:

i. Is there evidence whether developers of Mobile Health Applications generally apply responsible practices when collecting and using users' personal data?

ii. What would motivate developers of mobile applications to adopt a more responsible practice in collecting and using user data?

3.1. Action Plan

To answer the research questions, we undertake the following approach:

i. We analyze existing mHealth apps to identify evidence where excessive and unnecessary access to user private data is attempted:

a. We focus on the permissions requested by specific mobile apps. For this, we access data from the Android Ecosystem (i.e. we examine apps published on the Google Play market).

b. We analyze a subset of apps (35) which were selected because they show evidence of excessive access to user private data.

c. We examine how third-party components could also affect the resulting product. For instance, "… potential privacy and security risks [also] posed by embedded or in-app advertisement libraries" as it is stated by [4].

ii. We contact mHealth apps developers online to identify if they are familiar with, and apply responsible practices, and whether any form of accreditation would motivate them to adopt the RRI toolkit.

4. Issues in mHealth Apps Development

Over the years, mobile devices have continued to find their ways into, and revolutionize every sector of human life. The Health sector embraces a great number of mobile devices and applications that are being used in areas such as in checking of vital signs, in health records keeping and maintenance, diagnosis; in keep fit exercises and suggesting healthy diets, etcetera. The increase in availability of these smart devices causes a general increase in the incorporation of computing technologies into our professional, social and private lives. Unfortunately, the ubiquity of computing and smart devices comes with ethical issues and concerns especially in the area of dealing with user data privacy. We sought to find out if the developers of mHealth Apps adopt best practices in handling user data and whether the users themselves showed any concern about the privacy of their personal data being collected by the mHealth apps.

4.1. Ethics and mHealth Apps Development

Today, infrastructures handling critical jobs in our societies have an increasingly high degree of reliance on computing facilities which include both hardware and software. This could bring about ethical worries that were hitherto unanticipated. Ethics in computing is necessary therefore, as most times and in many areas and conditions, computer operations proceed invisibly; sometimes causing abuse or misuse of user data or not observing user privacy which could extensively impact the society. Legal issues relevant to computing and IT Professionals include Data Protection, online business practices (involving cookies and emails), Copyright & Patents, Accessibility, Libel, Negligence, Contract law and Computer crime. All infrastructures depending on computing to handle their critical areas needs to have its data integrity protected and build confidentiality in its information handling; as a result of which a lot of ethical issues could be raised. When computing devices are developed therefore, the developers need to put in place best practices to ensure that neither users nor the developers or even third-party applications (for example ad libraries) have unauthorized access to other users' personal data; and neither should any violate the ethics. The Ethics of computing are therefore required when developing mHealth apps.

[10] provided a systematic and comprehensive review of the literature on ethics of computing; giving a wide-ranging survey of the mainstream academic literature of the topic and discussing the general trends, arguing that it is now time to changeover to RRI; to ensure that ethical reflection of computing has practical and manifest consequences. They saw Ethics as a key component that can determine acceptance of new technologies and legislative and other responses to new technologies, even though they also noted that 'Ethics' could have many varying but interrelated meanings. Ethics basically, refers to the perception of an action as being good or right.

4.2. User Privacy and mHealth Apps Development

Privacy is seen as the dominant ethical concern and idea employed in computing world issues and; its frequent occurrence points to a diverse theoretic history and its being applied to technologies across decades, preceding 'computer ethics' as a discipline; [12]. Identity can refer to two broad areas of enquiry: firstly, as in 'identifiable information' concerning issues of data protection and anonymization; [6] and secondly, as a description of a person's sense of self which can be constrained in technologically mediated relationships, [8]; for example by constructing new informational representations of the user; [3].

5. Methods

Users of mHealth apps are required to grant certain permissions to the developers via the Mobile Apps store before the apps are downloaded and installed on their mobile devices. The permissions given by users provide the apps with access to specific capabilities or information on their devices, such as position, address book, etc. For example, users are shown which data an app would access from their devices when they preview such an app on Google Play. This information is intended to help users decide whether to install the app or not, depending on how reasonable the required permissions are to them. The most important permission groups normally appear on every download screen while the full list of permissions for an app may be found by following a link (usually provided by the developers).

We study the permissions users are required to grant before they could download and install mHealth apps on their mobile devices (with particular interest in personal data collection handling by developers). We also contacted developers and users of mHealth apps (via online questionnaires) to survey their level of applying responsible practice and showing concern on their personal data privacy respectively.

5.1. Data Collection

We collected thirty-five (35) mHealth apps from the Android Ecosystem and studied the permission requests by the apps to identify where an app attempts to make excessive and unnecessary access to user personal data. There are several mobile apps on the Google Play Store from where we identified the health related apps for the study. Different types of mHealth apps exist ranging from those used for fitness exercises to those used for health records and for diagnostic purposes. We collected information about user reviews on the 35 apps selected and their privacy policies from their respective web pages; and also contacted the developers to assess their level of awareness and adoption of Responsible Research and Innovation (RRI)practices in collecting and using user personal data when developing their apps. A Java program was written and used to crawl the apps sites for user reviews from where we try to check for user comments showing concern over their personal data; (Appendix 4). The Program uses the uniform resource locators (URLs) of the thirty-five (35) apps to trace all current "User Reviews" concerning them from the popular Google Play Store and save it to a text file. We then try to check out the comments in the reviews that suggest that the users are concerned about the privacy of their personal data. On the users review text file we use the 'Find' function, to search for key words such as 'private', 'privacy', 'concern', 'personal', 'data', 'information' and then check out the sentences where they appear. Most of the 35 apps collect data such as User Identity, Contact details, Calendar, Location (approximate and precise), Photos and Storage, Camera and Other Sensors. The analytical table of these permissions is presented in Appendix 1. We analyze user reviews on the apps to assess users' level of awareness of the fact that these apps collect such data from them; and how concerned they are about the privacy of their data being thus collected. There is no significant mention in the reviews by users of the apps to show that they are aware of, or that they are concerned about the privacy of their personal data being collected by mobile apps. This could be a result of one or more of the following possibilities:

i. The developers do not make the collection of user personal data explicit enough for the users to see and show concern about the privacy thereof.

ii. The users do not pay enough attention to notice that their personal data are being collected as they download and install these apps on their smartphones.

iii. Some users might have read up the Privacy Policies regarding the collection, management and use of the personal data collected by the apps and are comfortable with it.

iv. Users are aware of the fact that they cannot use the apps if they do not provide these data or grant the permissions for the apps to access them and so, they give in to good faith and release the information. This is especially true when they know that the apps are meant to be helpful for them.

Being that we did not find enough information on users' concern over their data privacy from the reviews, we went further to contact the users via online questionnaires. The data of the questionnaires are listed verbatim in Appendices Section (Appendix 5) and their analysis results are discussed in Results section.

5.2. Data Analysis

To find out if developers of mHealth apps apply responsible practice when developing their apps, we collected data from the apps privacy policy page where this is available. This helps to identify what type of data each app collects from its users and what privacy policies the app developers adopt to let the users know what is at stake (if any) when they place their personal data online to download and install the apps. We also examined the manner in which the developers relate with the users to access these data. In the first case, we try to know if the apps require permissions to collect such data as Identity, Contact, Calendar, Location, Photos and Storage, and Camera. In the second instance we try to find out whether these mHealth apps developers explicitly ask for user consent to collect user data and if they specify what type of information they collect from the users; whether they explain how they maintain privacy and security of user personal data and if there are clear mechanisms to unsubscribe and delete user personal data from their servers when required. We also try to find out if developers explicitly say whether they will sell and/ or share user data with third-parties; and if they have clearly spelt out Privacy Policies which users may use to understand how their data is protected. A detailed investigation leading to collection of data herein is included in Appendix 1. We also attempt to find out directly from the developers (via online questionnaires) whether they are familiar with, and apply responsible practice; and whether any form of incentives will make them more willing to adopt responsible practice. We sent out online questionnaires to the thirty-five (35) developers whose apps we study. Unfortunately we only had responses from three (3), the results of which are included in Figures 1-3. Results of the questionnaires also provided data for the question as to what would motivate developers to more readily adopt responsible practices.

In order to find out users' level of awareness of their personal data being collected when they install mobile apps and the privacy concerns thereof, we crawled user reviews for the apps (using a Java program, listed in Appendix 4) to see if they express concern over the privacy of their data. Unfortunately, this did not give much result. We therefore contact users of mobile applications online. We sent questionnaires to about 132 users and had responses from 39. The questions and results for the online survey are presented in the Results and Appendices sections respectively.

6. Results

This section lists the results collected via the different means described in Section 4.

6.1. Offline Analysis of App Permission Needs

Of the 35 apps selected, we reviewed the types of data the apps require permission to access from the users. The results are summarized in Table 1:

Table 1: Data Types required by mHealth Apps

S/No	Data Type	Required	Not Required	% Required
1	Identity	24	11	68.57
2	Contacts	23	12	65.71
3	Calendar	3	32	8.57
4	Location	19	16	54.29
5	Photos and Storage	31	4	88.57
6	Camera	22	13	62.86

Only three (3) out of thirty-five (35) apps analyzed (a very small percentage of 8.57%) require permission to access users' calendar while thirty-one (31) out of thirty-five (35) apps, representing a very high percentage (88.57%), require user permission to access user Photos and Storage. Twenty four (24) apps (68.57%) require permission to access user identity data. These are the data that identify the users and hence, their personal data. 23, 19 and 22 apps representing 65.71%, 54.29% and 62.86% require permission to access Contacts, Location and Camera respectively from the users' devices.

We try to study to further understand if users' personal data; including their identity, photos, locations (sometimes, even precise location) are so much required by the apps, do the developers do much on their own part to let the users know their apps would collect such information from them.

Here, we ask questions about developers' mode of collecting the information from users and whether they show in any way how this information will be treated. The results are presented in Table 2.

Table 2: Responsible Practices by Apps Developer

Answers to Responsible Practice questions	**Yes**	**No**	**% Yes**	**% No**
Do developers explicitly ask for user consent to collect User Data?	15	20	42.76	57.14
Do developers specify what type of information they collect from users?	30	5	85.71	14.29
Do developers explain how they maintain Privacy and security of user personal data?	14	21	40.00	60.00
Is there a clear mechanism to unsubscribe; and delete user personal data from their servers?	8	27	22.86	77.14
Do developers explicitly say whether they will sell/ share user data with third-parties	14	21	40.00	60.00

For twenty (20) of the thirty-five (35) apps reviewed, which is some 57%, their developers do not explicitly seek user consent to collect their personal data. The area where one could infer that developers collect data from users is mostly in the places where a whopping 85.71% require the users to grant permissions for the apps to access certain information before they are able to install them. Unfortunately, most times such language is not clearly understood by the users to mean that their personal data would be collected and stored away from their handheld smartphones. Developers of twenty-one (21) of the thirty-five (35) apps, being sixty percent (60%)do not say clearly how they maintain the Privacy and Security of User Personal Data; and another 60% do not clearly say whether they would sell/ share User Personal Data with third parties. For twenty-seven (27) apps of the thirty-five (35) which is 77.14%, users are not even given any chance to know if and how they may wish to unsubscribe and delete their Personal Data from the Servers where they have been collected and stored some far away from their mobile phones. About 54% of the developers of the mHealth apps under consideration put up some kind of Privacy Policies that give users the opportunity to read through and know everything surrounding the privacy of their data collected by the apps. Users however, do not always have the patience to read through these policy statements as most times they are not so precise and straight to the point.

6.2. Feedback from mobile app developers (via online questionnaires)

In the results of online survey to assess mHealth Apps Developers' familiarity with the concept of Responsible Research and Innovation (shown in Figure 1 below), 33% of the developers responded to positively while 67% are unfamiliar with Responsible Research and Innovation. The developers were also asked what usually motivates them to handle users' private data responsibly. The results presented in Figure 2 show that developers believe it is the right (ethical) thing to do. This suggests that if developers are aware of the things that constitute responsible practices, they would be more likely to abide by them.

Figure 1: mHealth Apps Developers Familiar with RRI

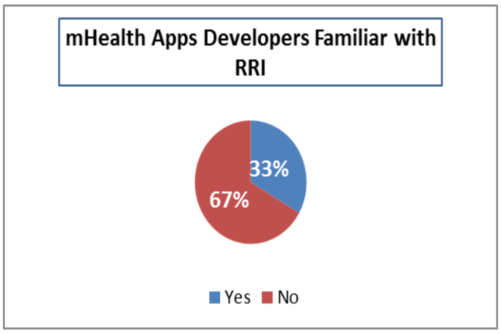
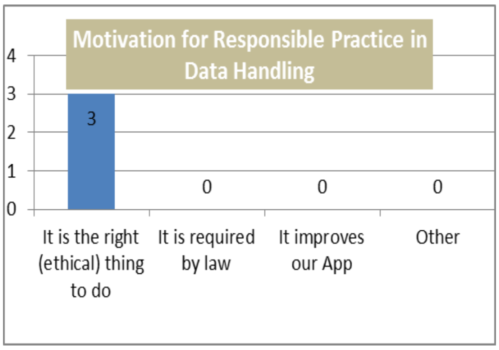
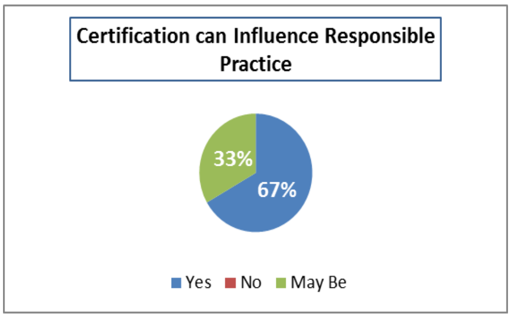


Figure 2: What Would Motivate Users to Handle User Private Data More Responsibly



As to whether there is a form of certification that would influence developers to take responsible practice in user private data handling more serious, we have 33% not being so sure while an overwhelming 67% answeredto the affirmative as could be seen in Figure 3 below:

Figure 2: Whether Any Form of Certification will Influence Responsible Data Handling



7. Discussion and Critical Evaluation

This study proposes that the adoption of responsible practices in mHealth app development remains inadequate and the level thereof varies from one developer to another.

Most of the Permissions required by the apps are not necessary for the purposes for which the apps are developed. For example, it does not make a lot of sense why an app which is developed to help users lose weight and monitor their blood pressure (such as Health Mate) would want to have access to the users' contacts. Since the contact details on the users' device wouldn't be used in tracking users' weight or monitoring their blood pressure, it can only be assumed that the developers will collect this data not for explicit use for the intended purpose for which the users are granting the permissions. Another case is that of an app, "Drugs Dictionary" which is a useful and friendly drugs dictionary and provides information about drugs: uses, dosage, side effects, precautions, drug interactions, and missed doses. Being that this app is just a drugs dictionary, its request for so much data from the users is rather questionable (e.g. it requires permission to collect user data including identity, contact details and both approximate and precise location. Data such as precise location and users' contact details do not appear to be relevant for such an app as a drugs dictionary which is just to be used by users to gather information about drugs, their dosage and side effects. We opine here that most developers collect some of these personal data from users' devices for uses other than the users would be willing, most likely for use with third-parties. This is in consonance with the opinion expressed by [4]. To answer the research question as to whether developers of mHealth Apps apply Responsible Practices while developing their apps, it is observed that most of the developers do not apply responsible practices. Most developers are not even aware of what responsible practices are and so cannot possibly be expected to apply the RRI kit.

Whether users are aware of the permissions they grant and if they show any concern about the risk of placing their personal data online is another question this study seeks to address. We find that most times users are not aware of the data which mobile apps are able to access from them when they grant permissions to install the apps. This position agrees with, and is a common theme in several opinions in the literature which expresses that the permission mechanism is rather complex and users don't usually understand the permissions they grant, [2, 3, 11, 12]. Although users do not show much concern in the user review sections during apps installation, in our online survey they claim knowledge of the permissions they grant when they install apps. Most users are also concerned about the privacy and security of their data. Unfortunately they say to have granted these permissions since they couldn't install the apps without allowing access to the required data. Also, it is found that developers would more readily adopt responsible practices in their developments of mobile apps if there were a form of incentives.

Of the 35 apps considered for this study, 31 (88.57%) require permission to access Photos and Storage on users' devices, 24 (68.57%) require permission to access identity, 23 (65.71%) require permission for Contacts, 22 (62.86%) require permission for Camera while 19 (54.29%) and 3 (8.57%) require permission to access Location and Calendar respectively. Apart from the permission to access Calendar that is required by a very small percentage (8.57%) of the apps analyzed, well over 50% of the apps require permission to access other user data that we queried. Since mHealth apps require so much permission to access data and capabilities on the users' devices, it is expected that Responsible Practices be so observed and user data be treated with all sense of decency. Both developers and users are supposed to know the issues at stake and to be in agreement when it comes to placing and collecting personal data online. Also, in trying to find out how well the developers handle their request for permissions to access user data we found that majority of developers of apps analyzed in this study (20 of 35 which is about 57.14%) do not explicitly ask to collect data from the users even though they do. The areas where most developers suggest that they collect data from users and specify the type of data (a whopping 85.71%) is in the places where they require the users to grant permissions for the apps to access such information before they are able to install them. Unfortunately, most times such language used in seeking these permissions is not clearly understood by the users to mean that their personal data would be collected and stored away from their handheld smartphones. About 60% of the mHealth apps developers do not show clearly how they maintain the privacy of user data and another 60% do not clearly state whether they would sell or share user data with third-parties. Less than 23% of the developers of the mHealth apps studied show clear mechanisms to unsubscribe and delete user personal data from their servers if the users so decide. Hence for the greater percentage of the apps, if the users decide not to use the apps again someday, their data continue to reside on the developers' database which is not supposed to be, especially without the consent of the users. The users are supposed to be the final point of control to their own personal data and decide whether or not they wish to delete their data from the developers' database whenever they wish to discontinue the use of any apps. There are a few cases where the developers show that they maintain the highest sense of Responsible Practice in their development via the way they handle user data. In one of such cases, developers of the app **Symptomate** Symptom Checker collect no personal user data for storage on their database. The app is an innovative symptom checker designed by doctors to help users find out more about symptoms of a wide range of ailments. It is said to have provided well over 500,000 health check-ups. Users enter basic information about their health complaints and receive a list of potential diagnoses and a recommendation of doctors they could contact. The app asks users a few carefully selected follow-up questions regarding their symptoms. It is driven by advanced artificial intelligence algorithm which uses a broad medical database of over 1000 symptoms and over 500 potential conditions. The medical database of symptoms is carefully created and curated by a team of experienced physicians. Another app that does not collect user data for storage in its database is the Health and Nutrition Guide. This app contains huge collection of Health Tips, Nutrition Tips, Nutrition Calculators, Home Remedies and Health Recipes which help users to maintain and improve their health and fitness. Only these 2 from amongst the 35 apps here analyzed (barely 5.71%) do not collect user data to store in their databases. Two other apps which also do not collect user data so vigorously but seeking permission only for access to user camera are Heart Rate Monitor and **Heartservice**. The dual are used for measuring user heart rate. Heart Rate Monitor is a cardiograph for user's Android device, giving results to enable users check their heart rates on real time basis. The app measures user's heart rate by analyzing blood flow on the tip of his/ her finger. Similarly, the **Heartservice** app uses medically correct methods to measure users' heart rate and heart rate variability using the camera of user's smart phone. For these two, it is understandable why the apps should need access to user camera. Four (4) apps (representing 11.43%) each collect at least a couple of the user data queried in this study but they also explicitly seek the users' consent and explain how they maintain user data privacy and if they share user data with third parties for any reason.

We see from this study that often mHealth app developers do not strictly observe responsibility practices in developing mHealth apps. This lack of adoption of Responsible Practice could be caused by different reasons including ignorance of Responsible Research and Innovation (RRI) on the side of some developers while others could be due to lack of incentives.

7.1. Developers' Ignorance of Responsible Research and Innovation

With the proliferation or spread of mobile devices and the capabilities these devices possess along with the realization of the fact that their developers could derive quite some financial benefits from them, so many people have moved into developing mobile apps. Most times, developers learn apps development but may not be familiar with the ethics and the laws that regulate those developments. They just learn the development skills and swing into action in apps development. We seek to know how well developers of the apps we analyzed are familiar with the principles of Responsible Research and Innovation. In Figure 1, we find that 67% of the developers who responded to our online survey are unfamiliar with RRI. Now, if such a large percentage of developers do not know the ethics and laws governing development of apps or those governing the handling of user data then, it is impossible for them to adopt and maintain responsible practice in collecting and using users' personal data during their developments. This also confirms that the adoption of Responsible Practice is inadequate.

7.2. Lack of Incentives for Developers

Lack of incentives could contribute to developers neglecting responsible practices during apps development exercises. We assume that developers of mHealth apps would be more willing to adopt responsible practices in their developments if there were some kind of accreditation to encourage them. We therefore move to find out from the developers of the apps we analyzed if there was any kind of incentive that would enhance their adoption of responsible practices. Incentives could come in form of financial benefits, recognition or any other form. We specifically sought to know if there was any kind of certification that would encourage the developers to adopt responsible practices. The results, as presented in Figure 3 show that 67% of the developers would be encouraged to adopt responsible practices if they could win some kind of certification while 33% were unsure. That none of the developers outrightly answered "No" to this, and the high percentage answering "Yes" proves that developers would be willing to improve on responsible practices in mHealth apps development if they are to be given some incentives. Another area to consider here is to think of penalties for developers who do not adopt responsible practices in their developments. Assuming developers knew they would be charged and fined to pay some huge sum of money (or any other penalty) for not imbibing responsible practices, they would probably not want to risk the fine as this would mean some financial loss to them and the processes involved in charging them and collecting fines from them may also affect their time and other resources.

8. Conclusions

We show that adoption of responsible practices in mHealth apps development remains low. We agree with [5] who decried the risks posed by these apps both on privacy and (sometimes) in mismanagement or mishandling of data, misinterpretation or misapplication of information. These could lead to incorrect health diagnosis and wrong treatments which can be quite dangerous to the users. On the other hand, we believe that if mHealth apps are developed responsibly and used appropriately, they would be of much benefit to the users and help them to live quite healthily. [5] also believes that the importance of Health Data goes beyond just healthcare and reaching forth to areas of human life such as insurance, etc. The present level of applying responsible practices by mHealth apps is inadequate and needs to be improved upon and doing this requires conscious efforts, both from developers and users of mobile applications as well as from governing authorities like the Government and Computing Professional Societies. The governing bodies should consider giving incentives to mobile applications developers who apply responsible practices while penalizing defaulters. Finally, the developers should be more professional and handle users' personal data more responsibly, knowing that users reveal these data details to them on trust. This agrees with the theme expressed in [9].

Developers especially, should apply responsible practices when they collect, store, manage and use users' personal data. Low level of adoption of responsible practices by developers of mHealth apps is seen in the fact that most of them do not do enough to inform their users of the data they collect from them, how these data would be stored, used and how they secure them. Developers need to be more explicit when asking for permission to access users' personal data and to show how the users may delete their data from the developers' databases if required. The study reveals that most developers do not adopt responsible practice in mHealth apps development due to ignorance of responsible research and innovation; while some would adopt responsible practice if there was some kind of incentives for applying responsible practices or if there was some kind of penalty against lack of adopting responsible practices in mHealth apps development.

9. References

[1] ALMUHIMEDI, H., SCHAUB, F., SADEH, N., ADJERID, I., ACQUISTI, A., GLUCK, J., CRANOR, L. and AGARWAL, Y., 2015. Your Location has been Shared 5,398 Times! A Field Study on Mobile App Privacy Nudging. CHI '15 Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems, pp. 787-796.

[2] FELT, A.P., HA†, E., EGELMAN, S., HANEY†, A., CHIN, E. and WAGNER, D., 2012. Android Permissions: User Attention, Comprehension, and Behavior, SOUPS '12: Proceedings of the Eighth Symposium on Usable Privacy and Security, July 2012 2012, ACM.

[3] FLORIDI, L., 2011. The Information Nature of Personal Identity.21(4), pp. 549-566.

[4] GRACE, M., ZHOU, W., JIANG, X. and SADEGHI, A., 2012. Unsafe Exposure Analysis of Mobile In-App Advertisements WISEC '12: Proceedings of the fifth ACM conference on Security and Privacy in Wireless and Mobile Networks, April 2012 2012, pp. 101-102-112.

[5] HUUSKONEN, P., HÄKKILÄ, J. and CHEVER, K.T., 2015. Who Needs a Doctor Anymore? Risks and Promise of Mobile Health Apps, MobileHCI '15: Proceedings of the 17th International Conference on Human-Computer Interaction with Mobile Devices and Services Adjunct, August 2015 2015, ACM, pp. 870.

[6] MIZANI, M.A. and BAYKAL, N., 2007. A Software Platform to Analyze the Ethical Issues of Electronic Patient Privacy Policy.33(12), pp. 695-698.

[7] MOOR, J.H., October 1985. What is Computer Ethics.16(4), pp. 266-275.

[8] MORDINI, E. and OTTOLINI, C., 2007. Body Identification, Biometrics and Medicine: Ethical and Social Considerations. 43(1), pp. 51-60.

[9] ORNSTEIN, C., 2016. Pro Publica. Doctors fire back at bad Yelp reviews — and reveal patients' information [online]. Available at:

[10] STAHL, B.C., TIMMERMANS, J. and MITTELSTADT, B.D., 2016. The Ethics of Computing: A Survey of the Computing-Oriented Literature

[11] TCHAKOUNTE, F., 2014.Research Gate. Permission-based Malware Detection Mechanisms on Android: Analysis and Perspectives

[12] WESTIN, A.F., 1970. Privacy and Freedom

[13] WIKIPEDIA, September 2014, 2014-last update, Best Practice [Homepage of Wikipedia], [Online]. Available: https://en.wikipedia.org/wiki/Best_practice [08/10, 2016].