ISSN 2321 -9017
Volume 7, No.1, December 2018 – January 2019
International Journal of Bio-Medical Informatics and e-Health
Available Online at http://www.warse.org/IJBMIeH/static/pdf/file/ijbmieh01712019.pdf
https://doi.org/10.30534/ijbmieh/2018/01712019

Mobile Health Applications Risk Management Framework

Benard Kipkoech[1], George Okeyo[2], Michael Kimwele[3]
[1]Jomo Kenyatta University of Agriculture and Technology, Kenya, benakipkoech@gmail.com
[2]Jomo Kenyatta University of Agriculture and Technology, Kenya, gokeyo@jkuat.ac.ke
[3]Jomo Kenyatta University of Agriculture and Technology, Kenya, kimwele@icsit.jkuat.ac.ke

ABSTRACT

Mobile health applications have transformed the delivery of health services globally, but they have also exposed their users to numerous risks. The mobile health applications industry can only achieve its full potential if its associated risks are well managed. This study investigated mobile health applications' risks and formulated a framework for a systematic approach in risk management. A descriptive study was conducted and questionnaire was used to gather primary data. The findings show that security and privacy breaches, reputation damage, fraud, poor clinical decisions and loss of doctor-patient assessment factor as the risks mobile health applications users are exposed to. The risk management framework consists of four domains: objective setting, threats and vulnerabilities identification, risk identification, and risk control and prevention measures.

Key words: Risk, Health apps, Risk management framework, threats, vulnerabilities.

1. INTRODUCTION

Mobile health applications (health apps) are software tools that can help users manage their health through a smartphone or tablet, ranging from simple diaries or reminders to more complex programs [1]. Their usage have become very popular and have proven to be of great benefit to healthcare sector. They are useful for diagnostics, behavioral prompts, reminders and continuous illness monitoring and self-management programs that extend beyond the boundaries of a physical clinic [2, 3, 4, 5]. For instance, a recent study found out that the use of mobile health apps could improve patient experience, especially with regard to accessing health information, making physician-patient communication more convenient, ensuring transparency in medical charge, and ameliorating short-term outcomes [6].

Despite the benefits of using health apps, their users have been exposed to numerous risks. First, security and privacy breaches have been highlighted by several studies as a risk health apps exposes to their users. For instance, through information security and privacy infringements, majority (95%) of the health apps pose at least some potential damage with minority (11%) posing potential damage [7].

Secondly, poor medical advice has been associated with usage of health apps which has led to low health quality services [8]. The ability of one to use a health app depends on number of factors namely: perceived ease of use, perceived usefulness, effectiveness, reliability, cost, awareness, user satisfaction and confidence [9] [10] [11]. A study proved that perceived ease of use and perceived usefulness of health app has significant impact on a person's intention to use the app [9]. The clinical decisions are being made based on the data collected from these apps regardless of the users' attention or intention when using the apps which has direct impact on the clinical decisions.

There have been various attempts by different bodies to manage the risks of health apps. The Food and Drug Administration (FDA) agency (US Food and Drug Administration Mobile medical applications: guidance for industry and Food and Drug Administration staff, 2013) and Health Insurance portability and accountability (HIPAA) act of 1996 (US Department of Health and Human Services, 1996) are some of the few bodies globally that monitor the usage of health apps in the health sector. FDA is only limited to mobile applications that are either intended to be used as an accessory to a regulated medical device or to transform a mobile app into a medical device while HIPAA regulates only mobile apps that are used in handling personal health information (PHI). HIPAA is limited to data privacy. This leads to two important questions. Where do health apps that do not fall into these categories go to? Who regulates these health apps yet it is well documented their usage exposes its users to risks?

In response to this, our study investigated the risks posed by health apps and formulated a mobile health applications risk management framework. The framework will provide guidelines on how stakeholders of health apps industry will manage the health apps risks.

2. RELATED WORK

2.1 Need for Health apps risk management

Risk management is a systematic approach for minimizing exposure to potential losses [12]. It is an important aspect in every industry if it has to strive to achieve its full potential. It is therefore crucial that a framework to manage health apps

risk is in place to safeguard the sector.

A study described a framework to assess risk and promote safe usage of health apps [8]. In the study, the researchers noted that there is currently no clinically relevant risk assessment framework for health apps, meaning healthcare professionals, patients and health apps developers face difficulty in assessing the risks posed by specific applications. The study identified several risks associated with using health apps, including:

- Hindering professional reputation;
- Causing possible patient privacy breaches;
- Resulting in low-quality service;
- Providing Poor medical advice.

The study further outlined some of the most common variables that can affect those risk factors, including:

- Apps that contain inaccurate or out-of-date information
- Inappropriate use by patients
- Inadequate user education.

Of those, the researchers warned that a lack of education poses the biggest threat to patient safety and recommended that health care professionals begin learning about the apps' risks before prescribing their use to patients. Overall, the authors called for a formal risk assessment framework for mobile health apps to help reduce the "residual risk" by identifying and implementing various safety measures in the future development, procurement and regulation of mobile apps. They argued that medical apps will flourish in the health care industry after a process has been created to ensure their quality and safety hence the need for health apps risk management framework to be put in place. The research, however, does not go further to demonstrate an elaborate framework to manage this risk but it only develops a risk assessment framework.

Another study on a conceptual framework for secure mobile health was conducted [13]. The study highlight security and privacy as major risk factors that can contribute to the failure of health apps. Health apps is depicted as a multidisciplinary healthcare delivery platform involving three elements technology, clinical and human factors. The researchers argue that since health apps industry is a multidisciplinary field, it is difficult to develop a comprehensive health apps risk management framework. Therefore, they proposed to have a risk management framework that works independently based on the three elements of health apps. The study mainly focuses on privacy and security as the major risk factors and aims to develop a risk based security framework for a balanced and effective approach to assessing designed considerations for health apps processes based on the three factors. However, good this proposed framework is, it does not address all the possible risks health apps expose their users to. It address only privacy and security risk.

According to another research, there is a significant rise on the use of mobile devices which has raised a concern on the data security and integrity [14]. The study further noted that there is lack of standardized data security to assure privacy, to allow interoperability, and to maximize the full capabilities of mobile devices presents a significant barrier to healthcare. Mobile devices security can be achieved through data encryption and secure communications. Mobile applications, however, raises a new challenge since the security of the data is purely dependent on the applications' developers. The study recommends a standardized secure mobile version of operating systems for use within the medical community.

Based on the researches outlined above, it is evident that health practitioners and health apps users find it hard to evaluate if health apps available for use are safe or not. This is further weakened by inexistence of legal regulatory framework to monitor these applications. There are thousands of health apps deployed by different developers which make it even harder to monitor these applications. If this not controlled early enough it may later escalate to adversely affect the health apps industry hence need for a risk management framework.

2.2 Health apps threats and vulnerabilities

There is need to understand the threats and vulnerabilities associated with mobile health applications in order to properly formulate a framework to manage mobile health applications' risks. The threats and vulnerabilities associated with usage of health apps are as listed:

1. Inaccurate and out-of-date app content

The health apps content ranges from medical prescriptions, informative, medical adherence to health and fitness instructions. These content may be inaccurate or out-of-date. The development of the mobile health industry has been driven by mobile network operators, app developers and device makers, with less buy-in by the medical fraternity [15]. This has raised concerns on the accuracy of content on health apps. In addition, health apps that contain inaccurate or out-of-date content have an increased chance of causing harm to their users [8]. For instance, a study found that a mobile app claiming to provide diagnostic recommendations for suspected melanoma had very low sensitivity and was therefore likely to miss many melanomas [16]. Use of this app had the potential to delay diagnosis and treatment for a condition in which early detection has a significant impact on survival rates.

Health apps content has been identified as one of the domains that needs to regulated [17]. Health apps and apps promotional content that contain easily accessible but inappropriate material may cause serious offence to or be

unsuitable for viewing by consumers (including children) and communities [17].

2. Inadequate user training

Health apps users require adequate user training to avoid the potential harmful or unsafe apps' usage [8]. The study shows that even when the health app user is used as the developer intended, risk can be increased if the user has inadequate training or knowledge to recognize when there is a patient safety hazard, for example, incorrect content or inappropriate advice from the app. Moreover, it is crucial to educate patients regarding the widespread of these unregulated apps as a result of the increasing frequency of patients presenting to their doctors armed with these questionable apps [18].

3. Inappropriate app usage

Health apps users have a tendency of using the apps in inappropriate manner which could cause serious harm due to absence of specialist(s) to provide assistance when using them [8]. For instance, insulin dosage apps have a tendency to be used inappropriately. A study demonstrated that Insulin dose calculators lacked user input validation and made inappropriate dose recommendations, with a lack of documentation throughout [1]. In addition, these apps may also be used inappropriately outside their design envelope intentionally or unintentionally [8].

4. Deployment of erroneous apps

Health apps will inevitability face technical problems that would arise during the system development process. Even the most careful coding will result in some "bugs" in products (e.g. errors, incompatibilities, unforeseen contingencies) [2]. In addition, the health apps' stores does not have a stand way of evaluating the presence of errors in the apps before deployment for public use. This is a source of threat to mobile health applications.

5. Apps malfunctioning

Malfunctions can potentially trigger damage both in the apps themselves (incorrectly implemented functionalities) and in the devices on which they are used [19]. Health app(s) can malfunction and there is no way for the users of health apps' to tell if the app(s) is functioning as intended. On the other hand, incorrect or misguided use (use-error) [20], for example due to design problems of the app in question, can be problematic. This can also occur if the app is used without being suited for the respective use case or if the requirements of specific usage scenarios were not given due consideration [20].

6. Malware and viruses

"Malware" is short for malicious software and is typically used to refer to a variety of forms of harmful or intrusive software, including computer viruses, worms, Trojan horses, ransomware, spyware, adware, scareware, and other malicious programs [21]. These malicious programs can perform a variety of functions, including stealing, encrypting or deleting sensitive data, altering or hijacking core health app(s) functions and monitoring users' computer activity without their permission [21].

The malware and viruses threats and vulnerabilities in health apps can be triggered by errors in code, incorrect logic, poor design, among other parameters [22]. They can also be either as a result of users' failure to install security software, device lose or stolen and lack of password-protection in devices [23]. Other health apps downloaded by users can be malwares and trick users into thinking that they have downloaded a legitimate app(s).

2.2 Risks of Health Apps

According to ISO 73, risk is defined as the effect of uncertainty on objectives. Therefore, the health apps risks are as a result of the execution of the threats and vulnerabilities which may negatively impact on the health sector. These risks are as follows:

1. Reputation Damage

Reputation damage risk refers to damage of one's reputation as a result of using health app(s). Health apps development has not been involving all the stakeholders yet the reputations of some stakeholders are at risk as a result of the apps' usage. In essence, the development of health apps has been driven by mobile network operators, app developers and device makers, with less buy-in by the medical fraternity [15]. Another study showed that lack of clinical trials during the development of health apps can result in inefficacy of the apps which proves the lack of medical fraternity involvement [24]. This may therefore, lead to unawareness of patient safety issues raised by inappropriate app. Furthermore, the reputation of health professionals who recommend or use health apps are put at risk yet they have not had hands on the effectiveness and reliability of the apps during their development [8].

Concerns for health professionals to be involved during the development of health apps have been raised. For instance, there is need for physician involvement in obtaining the app to boost the acceptability of the app by the users [25]. There is need to address this concern during the health apps development stage.

2. App usage Factor (AUF) risk

Any health app has a population of users and its usage frequency. App usage factor relates to the population of users and frequency of use of the specified app. The risk the health

apps expose their users is proportional to the number of patients affected and usage frequency, so disease prevalence or similar indices of the number of people likely to be affected by an error need to be considered [8]. This implies that in the event of errors in the app manifestation or malfunctioning, a large population of users would be affected.

3. Poor Clinical Recommendations

Health apps users rely on mobile devices and applications to collect information and make decisions that may be critical for the user's life and well-being [26]. This implies that if the data collected are inaccurate, then clinical decisions to be made by the health professionals can have a devastating effect on the health of the app(s) users.

4. Privacy and security breaches

Privacy refers to how people's data are collected, used and protected while security refers to protection of the data against disclosure to unauthorized users (confidentiality), improper modification (integrity) and accessible to the authorized users at any time (availability). A study found out that it is very crucial to have a proper management of personal health information collected by health apps [27]. The study noted that appropriate methods are not being taken by developers and to safeguard the health apps and as a result harmful apps are being released. In addition, privacy and security concerns on patients' clinical data have been widely acknowledged as being significantly critical to the widespread adoption of mobile technologies in various healthcare domains [28].

Several studies have revealed that the risk of data breaching is the most worrying and impeding aspect to health apps usage. A study showed that data breaches in healthcare are common where many doctors now are able to view patient's records without their knowledge which could further lead to medical identity theft [29]. Another study that analyzed 600 most frequently used apps, found that only 183 (30.5%) had privacy policies. Two thirds (66.1%) of privacy policies failed to address the app itself [7].

5. Loss of doctor-patient physical assessment factor

A thorough physical examination is an important ritual that benefits both patients and doctors [30]. It helps to satisfy a patient's elemental need to be cared for and a doctor's need to make meaningful observation from the patient to help make correct medical decisions [30]. Health apps usage leads to loss of doctor-patient physical assessment despite its vital role in patient treatment process [8]. The loss of doctor-patient physical assessment are a preventable source of medical error and adverse events are caused mostly by failure to perform relevant assessment [31].

2.3 Health Apps Risk Controls and Measures

The health apps risks can be controlled by implementing the following control and measures.

1. Data validation

Data validation is the process of ensuring data have undergone data cleansing to ensure they have data quality, that is, that they are both correct and useful. It is intended to provide certain well-defined guarantees for fitness, accuracy, and consistency for any of various kinds of user input into an application or automated system. Health apps collect data which is processed on the app or send to a central server for processing. The collected data are used as inferences to make decisions on the course of action to be taken on patients' treatments. The validation of the data collected by sensors in a mobile device is an important issue for two main reasons: the first one is the increasing number of devices and the applications that make use of the devices' sensors; the other is that also increasingly users rely on these devices and applications to collect information and make decisions that may be critical for the user's life and well-being [26]. It is therefore essential for data to be validated during collection and processing as this will ensure that accurate data are available from which inferences are drawn from.

2. Data encryption

Data encryption is a form of cryptographic mechanism which involves translating data into another form, or code, so that only people with access to a secret key (formally called a decryption key) or password can read it [32]. The cryptography is aimed at protecting data confidentiality, authentication, integrity, non-repudiation and access control [32].

In health apps, several security issues must be considered, such as personal information management, secondary use of personal information, improper use of personal information, and errors with stored personal information. Therefore, cryptographic mechanisms can be seen as a solution to guarantied data confidentiality and protection [33]. Data encryption in health apps allows users to safely obtain health information with the data being carried securely [34]. Therefore, there is need to ensure that health apps encrypted any data that is either stored or transmitted.

3. Use of antivirus software

Antivirus software is a type of software used for scanning, detecting and removing malicious software applications in computing devices such as mobile devices or computers. It is primarily meant to protect computing device against viruses such as spyware, malware or adware whose intention is to cause destruction to the computing devices or people using these devices either by destroying data stored or being

transmitted in computing devices or denying them access to the computing devices.

4. User training

Mobile health users with high levels of literacy results in better health outcomes [35]. A study showed that end-user training is positively correlated with both performance expectancy and effort expectancy [36]. In order to achieve better outcome in health apps usage, effective user training has to be done. Health apps are deployed for use with little knowledge by the relevant parties on whether the user guide will be sufficient. There are no sufficient ways of telling whether the user has correctly used the application are required by the developers.

5. Application testing and verification

Health apps need a thorough testing and verification to ensure they are free from errors before deployment for use. Health apps development and maintenance process has no regulation oversight hence the lack of adequate testing and verification. A Study recommended government regulation as an approach to improve the safety of medical apps [1]. There is need for all the relevant stakeholders particularly, the health professions to be well involved in the testing and verification of any mobile health application before use [1].

2.3 Gaps found in the literature review

Although there is significant progress in the development of health apps, it is evident that it poses a significant threat to the health sector. If these risks are not managed properly, then they can cause great destruction to the health sector. The following gaps were found in our literature review:

1. Health apps pose risks to the health sector. There is need for risk assessment and the threats and vulnerabilities associated with the risks to be clearly outlined.
2. There is need to outline the controls and measures on health apps should be implemented to curb the risks.
3. A risk management framework should be developed to act as a guide to managing the mobile health applications risks.

There is urgency for an elaborate health apps risk management framework to be in place to safeguard the health sector. Our study aimed to formulate a mobile health applications risk management framework.

3. METHODOLOGY

In this study, we used descriptive study approach. A survey of Kenyan health apps was conducted and primary data were collected using questionnaire. The questions were adopted based on the literature review.

The researchers administered the questionnaire over a period of four months on the selected Kenyan health apps organizations. This was done in two phases. Phase one was aimed at collecting data for formulating the health apps risk management framework while phase two data were to validate the proposed framework. Fifteen (15) health apps organizations were randomly selected to participate in the survey. Four users of the health app were provided by the selected organization to participate in the survey. In total fifty two (52) users were expected by the research to participate in the study.

The researchers then contacted the health apps organizations requesting them to participate in the survey. Those who responded positively were then emailed an online questionnaire which they were free to fill. The respondents were assured that all personal respondents would remain strictly confidential. Finally, thirteen (13) health apps organizations participated in the survey and thirty nine (39) completed questionnaires were received.

4. RESULTS AND DISCUSSION

The survey was conducted to investigate threats and vulnerabilities that exists in the health apps. The following results were found in the survey.

- Inaccurate and outdated app content: majority (59%) of the respondents agreed that inaccurate and outdated content is a health app threat and vulnerability. 35% of the respondents strongly agree while 6% were of a neutral option.

- Inadequate user training: more than half (58%) of the respondents agree that inadequate user training is a threat and vulnerability of health apps. Further 26% strongly agree while 16% voiced a neutral opinion.

- Deployment of erroneous apps: 50% of the respondents agree that deployment of erroneous apps is a threat posed by health apps while 26% strongly agreed. 18% took a neutral opinion while 5% disagreed.

- App malfunctioning: 49% of the respondents strongly agreed while 38% agreed that app malfunctioning is a threat and vulnerability to health apps. 14% presented a neutral opinion.

- Malware and viruses: 67% of the respondents strongly agree that malware and viruses is a threat and vulnerability to health apps. 31% agreed to malware and viruses to be a threat while 10% were voiced a neutral opinion with further 3% strongly disagreeing.

- App usage factor: 42% of the respondents agree that app usage factor is a threat and vulnerability to health apps.

16% voiced a neutral opinion while 21% strongly agreed.

From the above results, we recommend that the health apps risk management framework should adopt the following threats and vulnerabilities:

i. Inaccurate and outdated app content
ii. Inadequate user training
iii. Deployment of erroneous apps
iv. App malfunctioning
v. Malware and viruses
vi. App usage factor

The researchers sought to find out the risks that can result from execution of the health apps threats and vulnerabilities identified in the previous section. The following results were found from the survey.

- Reputation damage: 55% of the respondents agree while 39% strongly agree that reputation damage is a risk of health app usage. 3% of the respondents disagree with the remaining 3% of the neutral opinion.

- Privacy and security breaches: 58% of the respondents agree and 18% strongly agree that privacy and security breaches is a risk of health apps' usage. 5% disagree and 8% strongly disagree with 11% of the neutral opinion.

- Fraud: 27% of the respondents strongly agree and 38% agree to app usage factor as an effect of usage of health apps. 16% strongly disagree while 3% disagree.

- Loss of doctor-patient physical assessment factor: 27% of the respondents strongly agree that use of health apps led to loss of doctor-patient physical assessment factor with 43% agreeing. 14% strongly disagree while 16% were of a neutral opinion.

- Poor clinical decisions: 59% of the respondents agree that usage of health apps contribute to poor clinical decisions while 18% strongly agreeing. 16% disagree while 7% were of a neutral opinion.

From the above results, it can be observed that the health apps risks management framework should include the following risks:

i. Reputation damage
ii. Privacy and security breaches
iii. Fraud
iv. Loss of doctor-patient physical assessment factor
v. Poor clinical decisions

The researchers investigated the measures and controls that can be used to manage the health apps risks. The following results obtained from the survey:

- Data validation: majority (65%) of the respondents and 19% agree and strongly agree respectively that data validation acts as a control and measure in management health apps risks, with 3% preferring to be neutral with the statement.

- Data encryption: 42% of the respondents agree that data encryption is control and measure while 24% strongly. 13% and 10% of the respondents disagree and strongly disagree respectively with the statement.

- Use of antivirus software: 47% of the respondents agree use of antivirus software acts as a control and measure in health apps risks management while 21% strongly agree. 13% preferred to be neutral with 11% and 8% disagreeing and strongly disagreeing with the statement.

- User training: 42% of the respondents agree that user training act as a control and measure in health apps risks management while 37% strongly agree. 13% and 3% disagree and strongly disagree respectively with the statement.

- Application testing and verification: 47% of the respondents agree while 36% strongly agree. 11% of the respondents preferred to be neutral with each 3% disagreeing and strongly disagreeing with the statement.

From the above findings, the health apps risk management framework measures and controls should constitute the following:

i. Data validation.
ii. Data encryption.
iii. Use of antivirus software.
iv. User training.
v. Application testing and verification.

The research further sought to understand the reasons for implementing a risk management process by health apps organizations. The following results were obtained from the survey.

- Experience from previous attacks: 14% and 9% of the respondents agreed and strongly agreed that risk management were implemented as result of experience from previous attacks respectively. 36% disagreed with further 27% strongly disagreeing to the question asked.

- Enhance security of health apps: majority (91%) of the respondents agreed to implement risk management process in order to enhance security of health apps. 5% strongly disagreed with 5% presenting a neutral option.

- Prevent and control risks: 18% and 32% of the respondents strongly agreed and agreed to implement risk management process in order to prevent and control risks respectively. 23% disagreed with a further 5% strongly

disagreeing.

- Requirement by law: 36% of the respondents agreed while 27% strongly agreed to implement risk management process as a result of law requirement. 23% and 5% disagreed and strongly disagreed respectively to implement the process as law requirement respectively.

In the view of the above results, we recommend that the objectives of health apps risk management framework should:

i. Enhance health app security.
ii. Prevent reoccurrence of previous attacks.
iii. Evaluate existing controls and measures.
iv. Provide for legal compliance.

We aim at synthesizing from the discussions, analysis, and interpretations made so far in an attempt to establish a means that can help in evaluation, formation, and implementation of possible health apps controls and measures to address the situation observed and described in the previous section. Based on empirical analysis of existing risk management approaches and finding from the previous section, this work proposes a framework that can be used to manage the health apps risks. We recommend the framework to constitute the following domains:

i. A domain for outlining objectives of the framework.
ii. A domain for identifying threats and vulnerabilities.
iii. A domain for risks identification.
iv. A domain for risks control and prevention.

5. MOBILE HEALTH APPLICATIONS RISK MANAGEMENT FRAMEWORK

Our recommended health apps risk management framework as shown in figure 1 consist of four domains.

i. Objective setting
ii. Threats and vulnerabilities identification
iii. Risk identification
iv. Risk control and prevention measures

Objective setting domain

This is the first step in the risk management process. The risk management team sets out the objectives for the mobile health application risk management process. This is similar to the COSO framework objective setting stage. The objectives of risk management should be:

- Enhance Security
- Legal compliance
- Prevent reoccurrence of previous attacks
- Evaluate existing prevention measures and controls.

Threats and vulnerabilities identification domain

In this domain the threats and vulnerabilities that exist in health apps are identified. As identified from researcher findings, the risk management team should check on the following main threats and vulnerabilities in health apps:

- Deployment of erroneous apps
- App usage factor
- Inaccurate and outdated app content
- Inadequate user training
- Malware and viruses
- App malfunctioning

Risk identification domain

The risks that can result from the threats and vulnerabilities execution are identified in this stage by the risk management team. Based on the research findings, the probable risks that can result from the threats and vulnerabilities execution are as follows:

i. Reputation damage
ii. Privacy and security breaches
iii. Fraud
iv. Poor clinical decisions
v. Loss of doctor-patient physical assessment factor

Risk control and prevention domain

The existing controls measures are outlined each of the risk listed. Each control measured will be reassessed to see if it is sufficient to deal with the risk identified. The output will be a list of existing control measures as well as the proposed measures to counter the risks. The risks will be also gauged against the risk acceptance level to see if it is acceptable. The risks can either be avoided, reduced, transferred or accepted. Based on the researcher findings the following are the possible controls and measures that can be used to manage the risks:

i. Data validation
ii. Data encryption
iii. Use of antivirus software
iv. Application testing and verification
v. User training

6. CONCLUSION

Our main goal of the study was to formulate a mobile health applications risk management framework. In this study, we investigated the threats and vulnerabilities that exist in health apps and the risks they exposed their users to. We also extended our study to understand the objectives for implementing risk management process by health apps institutions and the controls and measures they can be used to manage the risks.

The findings of the study suggest inadequate user training, inaccurate and outdated app content, inappropriate app usage, malware and viruses, deployment of erroneous apps and malfunctioning of apps as the threats and vulnerabilities of health app usage. The findings also shows loss of doctor-patient physical assessment factor, reputation damage,

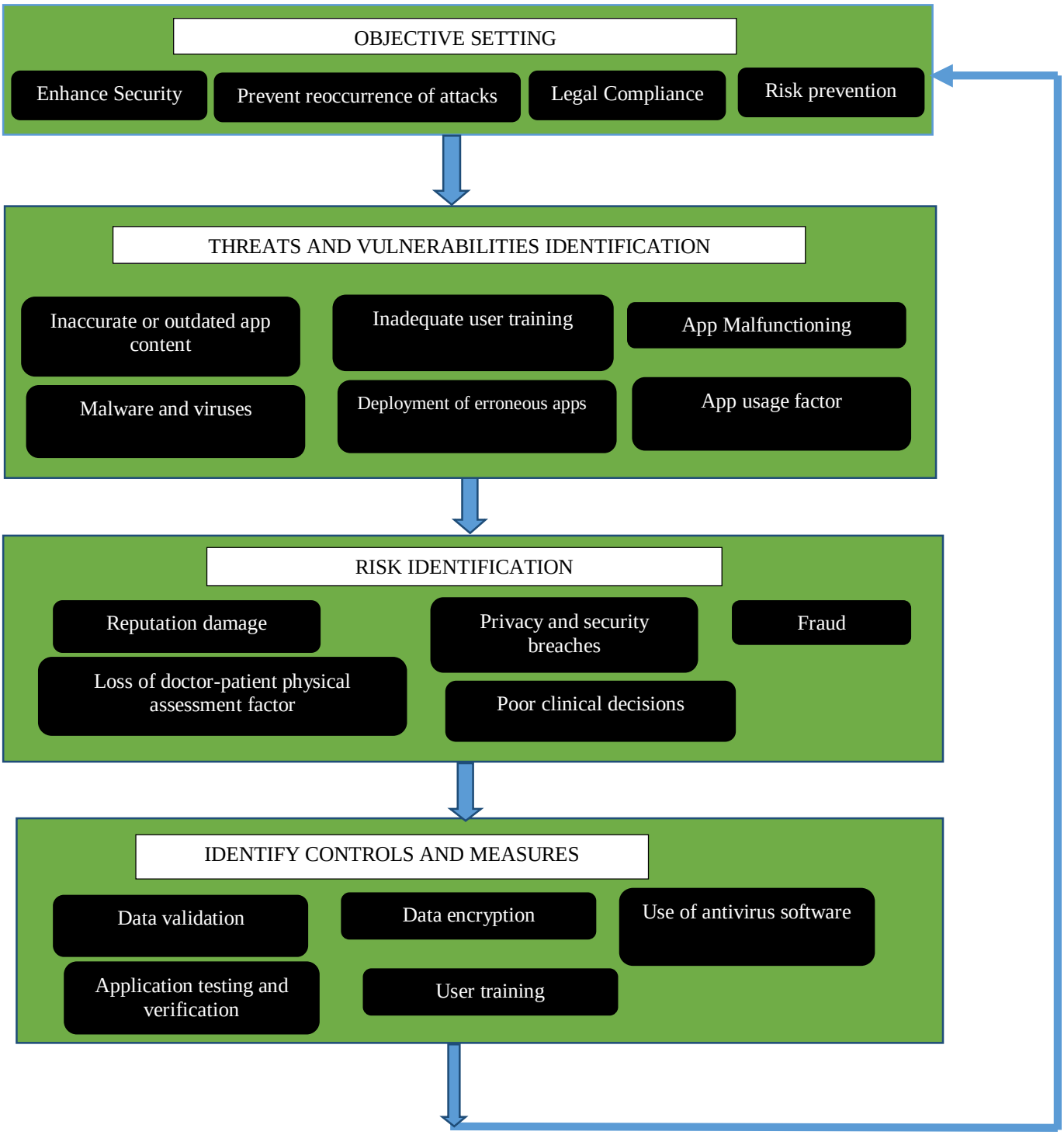

Figure 1: Mobile health applications risk management framework

privacy and security breaches, poor clinical recommendations and fraud as the risks health apps users are exposed to while using the apps. To prevent and control the health apps risks, data validation, data encryption, use of antivirus software, user training and application testing and verification were identified as the possible measures based on the study findings.

The findings of the study and the critical analysis of the existing risk management frameworks were used to develop the proposed mobile health applications risk management framework. The framework consists of four domains namely:

- Objective setting.
- Threats and vulnerabilities identification.
- Risks identification.
- Identification of risk controls and measures.

Each of the domain has a set of activities to be executed in the risk management process. These processes have to happen for effective risk management. The framework will help the stakeholders of health apps industry to manage the possible risks associated with their use. It equips them with a better understanding of the risks and provide a way of managing them. In general, safe health apps will promote the quality of health services.

7. FUTURE WORK

Since the framework has not been tested in a real working environment of health apps, further analysis on the effectiveness of the framework is required, and the results should be reflected in future frameworks.

REFERENCES

1. P. Wicks and E. Chiauzzi, "'Trust but verify' - five approaches to ensure safe medical apps," *BMC medicine*, vol. 13, no. 205, 2015. https://doi.org/10.1186/s12916-015-0451-z
2. D. Ben-Zeev, S. M. Schueller, M. Begale, J. Duffecy, J. M. Kane and D. C. Mohr, "Strategies for mHealth Research: Lessons from 3 Mobile Intervention Studies," *Springer US*, vol. 42, no. 2, pp. 157-167, 2015. https://doi.org/10.1007/s10488-014-0556-2
3. A. B. Labrique, L. Vasudevan, E. Kochi, R. Fabricant and G. Mehl, "mHealth innovations as health system strengthening tools: 12 common applications and a visual framework," *Global Health: Science and Practice*, vol. 1, no. 2, 2013. https://doi.org/10.9745/GHSP-D-13-00031
4. A. S. M. Mosa, I. Yoo and L. Sheets, "A systematic review of healthcare applications for smartphones.," *BMC medical informatics and decision making*, vol. 12, no. 67, 2012. https://doi.org/10.1186/1472-6947-12-67
5. G. Nasi, M. Cucciniello and C. Guerrazzi, "The role of mobile technologies in health care processes: the case of cancer supportive care," *Journal of Medical Internet Research*, vol. 17, no. 2, 2015. https://doi.org/10.2196/jmir.3757
6. C. Lu, Y. Hu, J. Xie, Q. Fu, I. Leigh, S. Governor and G. Wang, "The Use of Mobile Health Applications to Improve Patient Experience: Cross-Sectional Study in Chinese Public Hospitals," *JMIR Mhealth Uhealth*, vol. 6, no. 5, p. 126, 2018. https://doi.org/10.2196/mhealth.9145
7. T. Dehling, F. Gao, S. Schneider and A. Sunyaev, "Exploring the Far Side of Mobile Health: Information Security and Privacy of Mobile Health Apps on iOS and Android," *JMIR mHealth and uHealth*, vol. 3, no. 1, 2015. https://doi.org/10.2196/mhealth.3672
8. T. L. Lewis and J. C. Wyatt, "mHealth and Mobile Medical Apps: A Framework to Assess Risk and Promote Safer Use," *Journal of Medical Internet Research*, Vols. 16(9), e210, 2014. https://doi.org/10.2196/jmir.3133
9. M. R. Hoque, "An empirical study of mHealth adoption in a developing country: the moderating effect of gender concern," *BMC Medical Informatics and Decision Making*, vol. 16, no. 51, 2016. https://doi.org/10.1186/s12911-016-0289-0
10. N. F. Kiongo, "A framework for mobile health adoption in developing countries-case study Kenya.," 2014.
11. Y. O' Connor and P. O' Reilly, "Examining the infusion of mobile technology by healthcare practitioners in a hospital setting," *Springer US*, 2016.
12. C. J. Alberts and A. J. Dorofee, "Risk management framework," Software Engineering Institute , 2010.
13. P. A. Williams and A. J. Maeder, "A conceptual framework for secure mobile health," *Journal of the International Society for Telemedicine and EHealth*, vol. 1(1), pp. 44-51, 2013.
14. D. D. Luxton, R. A. Kayl and M. C. Mishkind, "mHealth Data Security: The Need for HIPAA-Compliant Standardization," *Telemedicine and e-Health*, vol. 18, no. 4, 2012. https://doi.org/10.1089/tmj.2011.0180
15. K. Laxman, S. B. Krishnan and J. S. Dhillon, "Barriers to Adoption of Consumer Health Informatics Applications for Health Self Management," *Health Science Journal*, vol. 9, no. 5, 2015.
16. J. Wolf, J. Moreau, O. Akilov, T. Patton, J. C. English, J. Ho and L. K. Ferris, "Diagnostic Inaccuracy of Smart Phone Applications for Melanoma Detection," *JAMA Dermatol*, vol. 149, no. 4, pp. 422-426, 2013. https://doi.org/10.1001/jamadermatol.2013.2382
17. L. Parker, T. Karliychuk, D. Gillies, B. Mintzes, M. Raven and Q. Grundy, "A health app developer's guide to law and policy: a multi-sector policy analysis," *BMC medical informatics and decision making*, vol. 17, no. 1, p. 141, 2017. https://doi.org/10.1186/s12911-017-0535-0
18. N. M. Hogan and M. J. Kerin, "Smart phone apps: Smart patients, steer clear," *Patient education and counseling*, pp. 360-361, 2012. https://doi.org/10.1016/j.pec.2012.07.016
19. G. Kemnitz, "Test and reliability of computers," Springer Berlin Heidelberg, 2007.
20. E. Israelski and W. Muto, Handbook of human factors and ergonomics in health care and patient safety, Informa UK Limited, 2012, pp. 475-506.
21. J. Aycock, Computer viruses and malware, Springer Publishing Company, 2010.
22. Y. Cifuentes, L. Beltrán and L. Ramirez, "Analysis of Security Vulnerabilities for Mobile," *International Journal of Health and Medical Engineering*, vol. 9, no. 9, 2015.
23. Z. Tu and Y. Yuan, "Understanding User's Behaviors in

Coping with Security Threat of Mobile Devices Loss and Theft," in *2012 45th Hawaii International Conference on System Sciences*, 2012. https://doi.org/10.1109/HICSS.2012.620

24. P. Krebs and D. T. Duncan, "Health App Use Among US Mobile Phone Owners: A National Survey," *JMIR Mhealth Uhealth*, vol. 3, no. 4, p. 101, 2015. https://doi.org/10.2196/mhealth.4924
25. L. W. M. van Kerkhof, C. W. E. van der Laar, C. de Jong, M. Weda and I. Hegger, "Characterization of Apps and Other e-Tools for Medication Use: Insights Into Possible Benefits and Risks," *JMIR Mhealth Uhealth*, vol. 4, no. 2, 2016. https://doi.org/10.2196/mhealth.4149
26. I. M. Pires, N. M. Garcia, N. Pombo, F. Flórez-Revuelta, Flórez-Revuelta and N. D. Rodríguez, "Validation Techniques for Sensor Data in Mobile Health Applications," *Journal of Sensors*, vol. 2016, 2016.
27. B. Martínez-Pérez, M. Lopez-Coronado and I. D. l. T. Díez, "Privacy and Security in Mobile Health Apps: A Review and Recommendations," *Journal of Medical Systems*, vol. 39, no. 1, 2014. https://doi.org/10.1007/s10916-014-0181-3
28. M. Farzandipour, M. i. Ahmad and F. Sadoughi, "Security Requirements and Solutions in Electronic Health," *Journal of Medical Systems*, vol. 34, pp. 629-642, 2010. https://doi.org/10.1007/s10916-009-9276-7
29. W. Figg and H. M. Kam, "Medical Information Security," *International journal of Security*, vol. 5, no. 1, 2011.
30. C. Costanzo and A. Verghese, "The Physical Examination as Ritual: Social Sciences and Embodiment in the Context of the Physical Examination," *Medical clinics of North America*, vol. 102, no. 3, pp. 425-431, 2018. https://doi.org/10.1016/j.mcna.2017.12.004
31. A. Verghese, B. Charlton, J. P. Kassirer, M. Ramsey and J. P. Ioannidis, "Inadequacies of Physical Examination as a Cause of Medical Errors and Adverse Events: A Collection of Vignettes," *The American Journal of Medicine*, vol. 128, no. 12, pp. 1322-1324, 2015. https://doi.org/10.1016/j.amjmed.2015.06.004
32. S. Kumari, "A research Paper on Cryptography Encryption and Compression," *International Journal Of Engineering And Computer Science*, vol. 6, no. 4, pp. 20915-20919, 2017. https://doi.org/10.18535/ijecs/v6i4.20
33. K. Raychaudhuri and P. Ray, "Privacy Challenges in the Use of eHealth Systems for Public Health Management," *International Journal of E-Health and Medical Communications*, vol. 1, no. 2, pp. 12-23, 2010 https://doi.org/10.4018/jehmc.2010040102.
34. B. M. Silva, J. J. Rodrigues, F. Canelo, I. C. Lopes and L. Zhou, "A Data Encryption Solution for Mobile Health Apps in Cooperation Environments," *Journal of medical internet research*, vol. 15, no. 4, 2013. https://doi.org/10.2196/jmir.2498
35. C. Z. Qiang, M. Yamamichi, V. Hausman and D. Altman, "Mobile Applications for the Health Sector," World Bank, Washington, 2011.
36. B. Marshall, R. Mills and D. Olsen, "The Role Of End-User Training in Technology Acceptance," *Review of Business Information Systems*, vol. 12, no. 1, 2008.