mHealth: Review of Security & Privacy Measures of mHealth Apps

by

Mancy Tomar

A Creative Component submitted to the graduate faculty in fulfillment
of the requirements for the degree of
MASTER OF SCIENCE

Major: Information Systems

Program of Study Committee:
Major Professor: Dr. Anthony M Townsend

Ivy College of Business
Iowa State University
Ames, Iowa
2021

TABLE OF CONTENTS

Page

ACKNOWLEDGEMENT

First and foremost I would like to express my sincere gratitude to my Major Professor Dr. Anthony M Townsend for his support and guidance throughout my graduate studies and related research for the completion of the Creative Component.

In addition, I would also like to thank my friends, colleagues, the department faculty and staff for making my adventure at Iowa State University a wonderful experience and for always encouraging me to push beyond my limits and providing me the timely guidance and insightful comments for my professional development.

Last but not the least, I would also like to thank my parents and brother for their continued faith, love, trust and support as I worked towards completing this important milestone in my educational career.

ABSTRACT

Mobile health (mhealth) apps are commonly used to keep track of our health, well-being, and everyday activities.They assist users with a variety of functions, including health tracking, understanding personal health issues, online doctor consultations, and achieving fitness goals. Although these apps provide easy access to healthcare, they do so by collecting, storing, and sharing a great deal of personal and confidential data about users. Personal information protection and privacy are major concerns when using mHealth apps.

This paper identifies the privacy threats and security features of mHealth applications, how they are assessed, and how the users perceive the privacy of mHealth applications, based on a literature review. According to the findings, providing a single mechanism for categorizing mHealth applications in terms of security and privacy is essential and beneficial.

1. INTRODUCTION:

1.1 Smartphone technology in Healthcare industry:

Smart mobile technology has made major inroads into society, with users ranging in age from school children to senior citizens in Western industrialised nations. Such development has been made possible by a long tradition of networking system use and widespread adoption**.** Because of their strong on-board computing capability, capacious memories, large displays, and open operating systems that enable application growth, the new generation of smartphones are increasingly regarded as portable computers rather than just phones (Maged, Steve, Carlos & Ray, 2011).

The use of mobile devices has grown exponentially due to rapid developments in mobile technologies. More than 70% of the world's population is expected to use mobile devices (Barboutov, Wallstedt, Torsner, Sveningsson, & Sachs, 2017). According to Economies and Markets (2020), the global mobile healthcare market will rise from $50.8 billion in 2020 to 213.6 billion dollars in 2025 (mHealth Solutions Market, 2020).

The introduction of mobile (m)health, smart (s)health, and electronic (e)health has been made possible by ever-increasing technological advancements in diverse fields. Smartphone devices and software (Apps) with internet access and collaboration capabilities, in particular, have appropriate channels. Currently, there are over 100,000 smart/mobile health apps available in the Android and iOS app stores. If technology and healthcare continue to advance in tandem, the number is expected to rise at an exponential rate (Faezipour, 2020).

Over the last decade, smartphone use and availability have increased, making mobile healthcare apps more available. Many of these apps enable users to monitor their habits and goals while on the go, as well as receive feedback and information (Petrizzo, Popolo, 2020). Smartphones already have a microphone for audio, a camera for image and video, gyroscopes for rotation and acceleration, and touch-screen fingerprinting biometrics, among other sensors. As a result, many physiological/biomedical data can be obtained directly from a smartphone device, which can then be processed and analyzed by an

app running on the smartphone's processor chip. To collect physiological data, some smartphone-based healthcare monitoring systems may require additional hardware and/or sensors that are wearable or connected to the smartphone device. Smartphones' integrated, real-time hardware and software co-design allows for fast integration and distribution of health-related data for continuous health monitoring. Furthermore, the smartphone's connectivity features enable the exchange of health-related data among users, patients, healthcare providers, and physicians (Kim, Campbell, de Ávila & Wang, 2019).

1.2.mHealth:

mHealth is a subset of the broader 'telehealth' term that refers to a specific way of utilizing mobile technology to achieve improved health care (World Health Organization, 2011). Telehealth refers to the use of electronic information and telecommunications technologies to exchange health information and provide health care services. Telehealth encompasses activities often termed telemedicine, telecare, among others(Scott, Mars, 1970). Live video conferencing, mobile health apps, store and forward electronic transmission, and remote patient monitoring (RPM) are examples of technologies used in telehealth. mHealth is defined as a medical and public health practice supported by mobile devices, such as mobile phones, patient monitoring devices, personal digital assistants, and other wireless devices (World Health Organization, 2011). Alternatively, mHealth is described as mobile and wireless devices used to improve health outcomes, healthcare services and health research (National Institutes of Health, 2015). mHealth has emerged as a segment of eHealth and encompasses mobile applications used for collecting clinical data, sharing healthcare information with practitioners, researchers and patients, real-time monitoring of patient health signs, and providing care and a platform for health workers' collaboration.

Mobile health apps are able to help people manage their own health, promote healthy living and have access to necessary information when needed. As of 2017, there are approximately 325,000 mHealth apps (Reports and Data, 2020). Google Play Store is home to more than 158,000 health apps- a 50% increase compared to 2016 (Pohl, 2020). There are over 43,000 apps on the iOS App Store alone, and

according to the Food and Drug Administration (FDA) mobile health (mHealth) apps were downloaded by 660 million people as of June 2013 (J. Conn, 2013)

There is immense opportunity for mHealth apps with the growing adoption of mobile technology in the healthcare industry. The global mHealth app market is projected to be valued at US $28.320 billion in 2018 and is expected to reach up to US $102.35 billion by 2023 with the increasing adoption of smartphones as well as continued investment into the digital health market (Research and Markets, 2017).

Without needing to make a prior hospital appointment, a patient may share his or her vital signs or lab results with medical experts all over the world using the pre-installed mHealth app. From a practical standpoint, mHealth tools, technology, and applications enable healthcare professionals to reach out to patients despite distance, time zones, and cost constraints.

Despite the competitive advantages and revenue generation, security of health-critical data is one of the most pressing challenges for the long-term viability and widespread adoption of mHealth apps(Bakheet Aljedaani, Aakash Ahmad, Mansooreh Zahedi, Muhammad Ali Babar, 2021).

Despite the potential effects of mobile health apps on patient health, there are no formal regulations or guidelines in place for their creation(Llorens-Vernet P, Miró J, 2020). This could lead to possible risks and low mHealth app quality. Some studies have found issues with current mHealth apps, such as their inability to address the needs of people with chronic illnesses (Giunti G, Guisado Fernández E, Dorronzoro Zubiete E, Rivera Romero O, 2018), a shortage of cited sources or references (Giunti G, Giunta DH, Guisado-Fernandez E, Bender JL, Fernandez-Luque L, 2018). In addition, there has been inadequate testing of mHealth apps in terms of usability and validity (de la Vega R, Miró J. ,2014). Such setbacks weaken the confidence of health-care professionals and patients in these apps (Huckvale K, Prieto JT, Tilney M, Benghozi P, Car J., 2015).

Privacy evaluation is a multifaceted topic that affects privacy policies, among other concerns mHealth apps' privacy policies provide privacy-related information that users should review prior to implementation to get a better picture of what personal data the app can access and when it will be

processed. These issues should be taken seriously, but a privacy policy is missing from 70% of the 600 most common health-related apps and many developers of these mHealth apps do not provide privacy policies in their apps either (Zhou L, Bao J, Watzlaf V, Parmanto B., 2019).

Over the past few years, scientists have been looking for a way to determine privacy in mHealth apps. Many studies have looked at app safety, with the majority of them concentrating on user interfaces, privacy in interactions, and privacy policies. The developed standards for evaluating privacy policies, on the other hand, are heterogeneous and subjective. These solutions are based on the researchers' own experiences, literature, and/or a legal system that already exists. The items used for the tests are varied, and the evaluation of these items is often subjective to the standards used by the evaluators. As a result, tools for evaluating privacy policies and establishing privacy scales based on objective standards that are less susceptible to interpretation are needed (Benjumea, J., Ropero, J., Rivera-Romero, O., Dorronzoro-Zubiete, E., & Carrasco, A, 2021).

Thousands of mobile healthcare applications exist, with around 40% of them specifically related to patient wellbeing and treatment (Constantino, 2013) Furthermore, neither the FDA nor any other entity regulates these apps. Android apps do not need to be approved, and any developer can publish their healthcare apps on the global market (Meier, R., 2012). This puts the app's users' privacy and security at risk by presenting false information and poorly developed functionality, it can also cause physical damage such as knee pain due to inaccurate advice by a diagnostic symptom checker app (Millenson, M. L., Baldwin, J. L., Zipperer, L. & Singh, H. Beyond Dr., 2017).

When selecting an app, users should make sure the information contained inside the app is complete and reliable, that the app is secure and well-supported, and that data protection safety measures are in place (Misra, S., Lewis, T.L., and Aungst, T.D., 2013). While there have been several demands for improved oversight of healthcare applications, nothing has been done to resolve these concerns (Visvanathan, A., Hamilton, A., and Brady, R., 2012). Because of the wide range of mHealth apps available, hackers and those with malicious intent can easily take advantage of and even damage

smartphone users (Felt, A.P., Finifter, M., Chin, E., Hanna, S., and Wagner, D., 2011). The current study adds to the body of knowledge by expanding on established theories about mHealth privacy and protection. A lot of research has shown that there is no unified way of assessing the privacy and security of mHealth apps largely due to the numerous categories of mHealth apps.

2. METHODOLOGY

This study helps us to get a sense of the various privacy and security issues that are present in the use of mHealth applications, as well as what steps can be taken to address them. The factors related to privacy concerns and security threats in the usage of mHealth apps, as well as the perception of mHealth applications users towards privacy and security , are described through a literature review. I looked at 38 different studies pertaining to specifically the privacy and security assessment of mHealth applications. I chose the studies that had a list of mHealth applications available in Android or Iphone or both and excluded studies that didn't do analysis of apps and gave a general framework for security assessment in the healthcare space. I obtained these studies from Iowa State online library, NIH and Google scholar by searching for keywords like "mHealth". "Mobile health applications", "privacy", "security" , "mHealth applications", "user-perception", "end-user perception" and combining these keywords using "AND" operator to give a result containing studies pertaining to privacy and security of mHealth applications.

3. LITERATURE REVIEW AND RESEARCH QUESTIONS

The purpose of this paper is to concentrate on the concerns around privacy vulnerabilities and security threats associated with the use of mHealth apps. The literature review was aimed at uncovering answers to the following questions:

R1: What variety of methodologies are used to assess the privacy and security concerns of mHealth applications?

Discussion about R1. Therefore, I form my first hypothesis:

H1: There is one unified way of assessing privacy and security concerns of mHealth applications.

R2: What are currently the most common security and data privacy issues involved in the use of mhealth apps?

Discussion about R2. Therefore, I form my second hypothesis:

H2: Data sharing by third parties is problematic and violates privacy.

R3: How is the privacy of mHealth apps being perceived by end-users?

Discussion about R3. Therefore, I form my third hypothesis:

H3a: Although applications have privacy policies, one of the reasons end users are not aware of privacy policies is because app developers do not make this information transparent.

H3b : Although applications have privacy policies, end users are not concerned with them and do not seek out this information voluntarily.

Various literature was found on the different aspects of mHealth applications, which are discussed one-by-one below:

App Discovery/Identification and Selection (Addresses R1)

Various literature points out a common theme for mHealth app identification and selection. Apps belonging to the medical, health and fitness category were selected. Apps were identified with keywords containing the root words “medical,” “health,” “fitness.”

Some studies were specific to a certain functionality or medical condition like cancer and used search strings such as“cancer mama,” “cancer prostata,” “cancer,” “cancer color recto,” cancer pulmon” (Benjumea, Ropero, Rivera-Romero, Dorronzoro-Zubiete, & Carrasco, 2020).

One study chose all mobile apps available in the NHS Health Apps Library in July 2013 available in Android and iOS (Kit, Jose, Myra, Pierre, & Josip, 2015). Another study identified 38 apps to review based in a list of top healthcare apps from a report created by IMS Institute for Healthcare Informatics(Miloslava, Steven, & Samir, 2015). One study focused specifically on mHealth apps for diabetes and blood pressure and included 154 apps (55% diabetes, 35 % blood pressure and 10% both) for analysis (Konstantin, David, &Maria, 2015).

There was a study that focused on self-tracking apps from the Google Play store and chose 292 apps after ranking the survey responses of 105 members of the London Quantified Self Meetup Group based on keywords such as “weight,” “sleep,” and “mood” (Hutton, et al., 2018). Most of these apps are available only in English; however, one thing to note is that where the studie are conducted influences the languages-apps are available in. For instance, one study was conducted in Spain and included cancer monitoring apps that were available in English and Spanish (Benjumea, et al., 2020).

Multiple researchers followed a similar approach when selecting apps to use in their studies. Many of these researchers (Benjumea, et al., 2020); shared in their methods section how they selected the apps. This includes:

- Identifying the highest number of downloads on the mHealth market
- Identifying high ratings from consumers, search engines or Android and iOS mobile app stores, and apps recommended by social media

- Having availability of apps in English
- Having availability of apps for free or less than $50 per subscription

The apps that were excluded from the study exhibited criteria such as not matching distinguished tags, not offering English descriptions or not having health-related functionality. Apps were also excluded if they would not start after two attempts on different test devices. Free demo and 'lite' versions of apps were also excluded if a full version of the app was available (Kit, et al., 2015).

Static Analysis (Application Permission) (Addresses R1)

Static analysis can be done using tools like MobSF or MalDroid to analyze the information in the apk file of the application. Apk file generates analysis of information like application permission by reading SD card contents, viewing network status, GPS location, viewing Wifi Status. APKID is an Android application identifier for packers, protectors, obfuscators and oddities (Zhao, Shahrair, Clincy, Bhuiyan, 2020).

MalDroid was used in one of the studies to identify SSL usage, like failure to check certificate chains which would allow man-in-the-middle attacks that enables an attacker to access all medical transmitted data.

OpenSSL was used to extract certificate information and find certificates with badly chosen cryptologic parameters. Drozer was used to search Android content providers and debugging flags. With its ContentProvider class, data can be shared between applications using its own type of access control. Unauthorized access to confidential data can be avoided with careful implementation. When the debug flag for Android is set, the app can be debugged even if it is running in user mode, potentially exposing medical information.

The add-on libraries used by the apps were identified and classified using Addons Detector. Snoopwall Privacy App, Clueful, AVG Antivirus Security, AVAST, McAfee, and the Recap vulnerability scanner were used to search health apps for malicious code, security vulnerabilities, and privacy flaws.

Code quality can be evaluated by counting the number of likely-bug patterns that appeared in apps using FindBugs; high numbers suggest likely poor code quality, which could lead to unstable conduct, posing additional security and safety risks (Knorr, Aspinall, Wolters).

Dynamic Analysis (Addresses R1)

Similarly, MobSF is used to conduct dynamic analysis. While monitoring code, dynamic analysis examines relevant functions such as register contents, function execution performance, memory use, and so on. It also examines the function of functions, clarifies code logic, and uncovers potential vulnerabilities.

AVD (Android Virtual Device) was used in one study to run the application to incorporate dynamic analysis. To simulate the AVD, Genymotion was used . MobSF could achieve real-time monitoring of the application by using an application on the Genymotion emulator. It displays the classes and methods that an application uses to interact with the device's various systems (Zhao et al., 2020).

Dynamic analysis can also be done to test for abnormal or illegal inputs and to assess how the exported data was stored or transmitted. One study used an Android debugger command adb pull and adb logcat to test whether the backup or log data contained unencrypted medical data and established whether the app included a feature to erase all stored medical data, whether there was a privacy policy for the app and if permissions required by the app were reasonable (Knorr et al).

Web Server Connection (Addresses R1)

A study checked if a sensible password policy was implemented on the web site and tested the Web Server link for apps that can communicate with a dedicated web server (n=20) using a user account for uploading data. URLs used for connections were recorded, as well as whether or not they used secure transport (https:). Web traffic was monitored to see if passwords or medical information in textual or graphical form could be sniffed in clear text (Knorr et al).

HTTP Analysis (Addresses R1)

One study conducted an HTTP analysis by testing the web server configuration to check the security of data transmission. By using a tool- Qualys SSL Labs to analyze the server of the application and show security level through a letter grade.

SSL Labs begins by examining the webserver's certificate, which is used to mark the server. After that, it runs a series of checks, like Protocols: A compilation of rules that must be followed by all sides of a communicating computer. Cipher Suites are a concept in the TLS/SSL network protocol. TLS 1.3's cipher suite specification has been modified such that it is only only used to negotiate encryption and HMAC algorithms, Handshake Simulation: Simulation of the process of Handshake. Until information is exchanged in data communication, the sequence of events handled by hardware or software must agree on the state of the operation mode. It is the method of establishing communication parameters between a receiving station and a transmitting station; HTTP Requests: a request sent by a client to cause a server to perform an action (Zhao et al).

Readability Analysis (Addresses R1)

Readability is one of the parameters by which understandability of privacy policy is measured. Readability test can assess the difficulty of vocabulary and sentence structure in English written material. It has been challenged as it can only measure the surface characteristics of text and does not measure qualitative factors such as reader’s interest, sentence, composition, structure, vocabulary selection and overall comprehensibility of the text. Document for health or safety instructions are recommended to be written at a 5th grade level (Dubay, 2004). One study selected Text-Statistics for privacy policy readability testing. Flesch-Kincaid Reading Ease (FKRE) score based on 0-100 scale grade level indicating an approximate representation of grade levels in the US public schooling system was used. The Simple Measure of Gobbledygook (SMOG) Index was also used for assessing the readability of

health care related materials and the reading grade level averages indicated that many of the privacy policies are written above the 12th grade level (Rowan, Dehlinger, 2014).

Privacy Policy Analysis (Addresses R1)

Privacy policies are statements or legal documents that describe how a mobile app can obtain, process, and share personal information from its users. Users may understand the potential for an app to manipulate their classified information by reading privacy policies, as well as any controls given to enable or limit such access (Bakheet, Ahmad, Zahedi, Babar, 2021).

A number of different studies assessed the in-app documentation of privacy policies of the apps and visited the related websites to study privacy related texts. Most common issues related to privacy include unauthorized collection of data, data breach, data storage and data sharing mechanisms. A lot of literature also pointed to a common theme of establishing a comparative analysis of selected apps in the medical category and giving the various parameters used for assessing privacy policies a score. So if the parameter was present in the privacy policy,it was awarded a point and if the parameter was absent, it scored a zero. This score helped compare how different apps differed in terms of risks that they exposed the users to (Sampat, Prabhakar, 2017).

Table 1 shows a summary of comparison analysis of 20 mHealth apps. Out of 20 apps only one enables the customer to delete personal information completely. Just 5% of the applications, or one, listed that users could fully erase their personal information. According to the study, 65 percent of the apps (13 apps) required users to enter personal information such as name, address, email, and date of birth, but only two apps required users to authenticate before logging in.

Half of the applications (50 percent, or ten) stored data in the cloud, posing major threats to customers' data privacy, and 65 percent, or 13 apps, shared users' data with a third party or advertisers. Just 20% of apps (or 4) told users about data privacy and security measures; however, 90% (or 18) of apps

have a privacy policy that outlines the app's privacy and security measures in detail (Adhikari, Richards, 2014).

	* registration	* cloud storage	* third party	authentication	update profiles	complete delete	local data	security explained	privacy policy	*risk score (3)	safe score (6)
Myfitnesspal	1	1	1	-	1	1	-	-	1	3	3
Medscape	1	1	-	1	1	-	-	1	1	2	4
Epocrates	1	1	1	-	-	-	1	-	1	3	2
Neuromind	-	-	-	-	-	-	1	-	1	0	2
Smart Bp	-	-	-	-	-	-	1	-	1	0	2
Pill Monitor	-	-	1	-	-	-	1	-	-	1	1
Pregnancy & Baby	1	1	1	1	-	-	1	-	1	3	3
Diabetes Tracker Plus	1	-	-	-	1	-	1	-	1	1	3
Growth	1	-	-	-	1	-	1	-	1	1	3
Instant Heart Rate	1	-	1	-	-	-	1	-	1	2	2
Ob (Pregnancy)	-	-	1	-	-	-	1	-	-	1	1
Calorie Counter	1	1	1	-	-	-	-	-	1	3	1
Skyscape	1	1	1	-	1	-	1	1	1	3	4
Endomondo	1	1	1	-	-	-	-	-	1	3	1
Itriage	1	1	1	-	1	-	-	1	1	3	3
Appointuit	1	1	1	-	1	-	-	1	1	3	3
Cardiograph	-	-	-	-	-	-	1	-	1	0	2
Quit Now	-	-	1	-	-	-	1	-	1	1	2
Gi Monitor	1	1	1	-	1	-	1	-	1	3	3
Stress Check	-	-	-	-	-	-	1	-	1	0	2
Total	**13**	**10**	**13**	**2**	**8**	**1**	**14**	**4**	**18**		

Table 1: (mHealth App Comparison Results, Adhikari, Richards, 2014)

R2: Privacy and Security Threats in mHealth app usage

Privacy Risks/ Threat (Addresses R2)

Users' personal information is shared via mHealth app stores, and users' lack of familiarity with the app environment leads to a slew of privacy issues. mHealth has enabled consumers to monitor their own health, resulting in a move away from medical offices and toward smartphone apps and cloud storage, raising several privacy and security issues(He et al., 2014). According to the National committee on Vital and Health Statistics (NCVHS), "Health information privacy is an individual's right to control the acquisition, uses, or disclosures of his or her identifiable health data. Confidentiality refers to the obligations of those who receive information to respect the privacy interests of those to whom the data

relate. Security refers to physical, technological, or administrative safeguards or tools used to protect identifiable health data from unwarranted access or disclosure" (NCVHS, 2006). According to a study of 43 fitness apps, 74 percent of free apps and 60 percent of paid apps had a privacy policy that could be found in the app or on the developer's website. According to the study, only 25% of free apps and 48% of paid apps informed users about their privacy policies (Mc Carthy, 2013).

Access Threat/ Control/ Informed Consent/ Privacy Policies (Addresses R2)

In the context of mHealth applications, informed consent refers to patients' or their legal representatives' permission to share their personal information when and with whom it is shared(Anaya,A, N, Prasad, 2018). Consumers are often unaware of all of the ways in which a service can capture and analyze their data, as well as the degree to which their data can be shared with third parties (Mense, Steger, Sulek, Jukicsunaric, Mészáros, 2016). As a result, the importance of transparency cannot be overlooked. Where privacy policies do exist, they are often non-specific to the app in question, do not notify users when the policy is changed or whether their data is to be exchanged, do not provide users with the ability to access their personal data, and are otherwise HIPAA non-compliant(Minen, Stieglitz, Sciortino, Torous, 2018). In a recent analysis of mHealth apps, it was discovered that a number of them requested "dangerous" permissions to access areas involving the user's private information or stored data, including those that were beyond the reach of the apps, such as the use of the microphone, Bluetooth communication, the user's contacts or calendar. Papageorgiou,Strigkos, Politou, Alepis, Solanas, Patsakis, 2018).

Poor Data Collection/ Improper Storage mechanism/ Poorly Protected consumer Data (Addresses R2)

Only 183 (30.5 percent) of the 600 most commonly used apps had privacy policies, according to a survey. Two-thirds of privacy policies (66.1%) did not mention the app itself (Sunyaev et al., 2015). Open platforms for app development have privacy policies that do not discuss the app directly. The privacy

policies that were available were not transparent to users in terms of their privacy practices, required college-level literacy, and were often not centered on the app. Developers either fail to inform users of how their personal data is used or demand excessive quantities of personal data from them (Ackerman, 2013). According to the Pew Internet Survey, 54% of app users opted not to install a mobile phone app after learning how much personal information they would have to share in order to use it. Similarly, 30% of app users have uninstalled an app that was already installed on their phone because it gathered personal details that they did not want to share. Not all apps have taken the requisite measures to safeguard confidential information about sexual activities and partners, as well as information about reproductive functions (Lupton & Jutel, 2015).

Data Encryption (Addresses R2)

Encryption is the process of converting data into a format that is incomprehensible to unauthorized individuals. As a result, mHealth apps that do not encrypt user data could pose a risk to data privacy. Nasiri (HealthCareBusinessTech 2014) also mentioned the dangers of mHealth apps in terms of data privacy. He discovered that many people use mHealth apps to communicate with their doctors, as well as monitor and handle symptoms and other information. Consumer information exchanged with others, according to Nasiri, can pose a privacy risk. According to him, researchers conducted a survey of 20 of the 23 most common free mHealth apps and discovered that 50% send data to third-party advertisers and 39% send data to unidentified parties without encryption. In certain respects, he claims, paid mHealth apps are better than free mHealth apps. Many free mHealth applications for mobile send data, link to third-party sites, use unencrypted connections, enable third-party data collection, and store data in the cloud. The majority of the time, this occurred without users being informed.

A study by Knorr, Aspinall stated that health data encryption is almost never provided.

Just one of the applications they reviewed allows the user to access medical records, maps, and tables. Since most apps allow users to send e-mail or save data to an SD card, medical data is not covered when exported or sent (or relies on other Android protection mechanisms).

Device Vulnerability (Addresses R2)

According to a report, 31% of mobile phone owners have lost or had their phone stolen, and 12% of mobile phone owners report that another person has accessed their phone's contents in a way that made them feel their privacy has been violated. Many people backup their phone data as a precaution in case their phone is lost or stolen. Despite the fact that backing up one's phone is usually done as a precaution in the event that it is lost or stolen, mobile phone owners who have had their phone lost or stolen are no more likely than the average to back up their phone's contents (Pew Internet Report).

Data Security breaches (Addresses R2)

Healthcare data breaches are widespread, with many physicians being able to access patient records without their knowledge, potentially leading to medical identity theft (Figg & Kam, 2011). Medical identity fraud, according to the World Privacy Forum, occurs when someone uses another person's identity, such as a person's name or Medicare number, without that person's knowledge or permission, posing a security risk to many customers. (Dixon et al., 2006). Between 2005 and 2011, the US Federal Trade Commission (FTC) reported nearly 18,000 cases of medical identity theft. Theft of a medical identity could result in the perpetrator receiving some unauthorized benefits. The perpetrator can steal medical records to sell on the black market or change them for fun, such as adding false diagnoses, blood types, drug allergies, and other health details.

End-User attitude towards Privacy (Addresses R3)

User attitude towards privacy of personal health data is widely variable. Data privacy and protection is cited as a primary concern or importance in some studies (Anaya, Alsadoon, Prasad, 2018), while users showed little concern in others (Ostherr, Borodina, Lotterman, Storer, Williams, 2017). Other researchers noted this disparity in their findings, with some participants voicing serious privacy concerns and others claiming it was not a problem(Cheung, Bietz, Patrick, Bloss, 2016). While some users raised concerns about the collection of highly sensitive data, such as information about mental health, reproductive health, or HIV status(Bucci et al, 2018; Zhao, Zhu et a, 2018l; Ronen, et al, 2018; Stawarz, Priest, Tallon, Wiles, Coyle, 2018; Campbell, et al, 2017)], others who provided such information expressed little concern about their privacy (Biswas et al ,2017). Even those who are concerned about their privacy may not want to thoroughly educate themselves about the dangers of disclosing and sharing their data through the use of a mobile health app or service, due to the ambiguous language and lengthy format of such privacy policies. Users do, however, often request more choice and control over their data, and app developers struggle with how to enable and handle those granular controls according to usability heuristics. Furthermore, users seem to be recognizing that aggregated pseudonymized data might not be as private as previously believed(Leinbenger, Mollers, Petrlic, Sorge, 2016), posing additional challenges to vendors and data brokers to consider privacy protections related to big data.

End-User awareness towards mHealth Apps Privacy policies(Addresses R3)

End-users are usually provided with privacy policies prior to the installation of mHealth apps. End-users' lack of understanding of privacy policies can be attributed to:

(i) mHealth app providers' lack of clarification and openness in addressing such policies, or

(ii) end-users' failure to read through such policies to understand their implications. (Plachkinova, Andres, Chatterjee, 2015; Parker, Halter,Karliychuk, Grundy, 2019)

Content review was used in a study to look at privacy issues for 61 mental health applications. The study's findings indicate that privacy policies are often vague, and that end-users should be informed about how and when their health data is obtained, stored, or shared with third parties.The majority of the examined apps allow end-users to post health-critical information on social networking sites without considering the social and legal implications (Parker et al, 2019).

Furthermore, privacy policies are often framed in such a way that they are difficult to read and comprehend due to the use of complicated terminology and notations. Another research looked at user views on mHealth applications, specifically for bipolar disorder patients. Participants in the study indicated that they had no qualms about upgrading software or purchasing features that will help them protect their privacy. End-user privacy awareness must be raised, and mHealth organizations can promote the clear presentation of privacy policies as part of user training to accomplish this(Plachkinova, et al, 2015; Parker et al, 2019).

End-users' concern towards mHealth Apps data privacy (Addresses R3)

Health data privacy ensures that confidential information is kept private and only exchanged with entities (humans or computer systems, for example) who are authorized to see it. The features to ensure protection of their health data and private information were mentioned by 13% of the respondents in the study. Concerns about data protection involved the disclosure of personal information without authorization and the use of that information for commercial purposes. In the event that private information is accessed by a third party, the respondent suggests proper warning or warnings. *'Notify access warning via application or SMS,*' one user wrote. End-users are concerned about securing private data and protecting its protection from other humans or non-humans, such as third-party programs that sense users' location and context. According to the results of a survey, some users shared their dissatisfaction with the fact that all medics (manager level users of the app, e.g., nurses, physicians, technicians), regardless of their medical background, have access to health critical information of any patient. Furthermore, managerial level app

users' access rights can be expanded outside working hours and health unit premises. This raised questions about the safety of users' health-critical data (symptoms of illness, medical images, and so on), which could be leaked and have social consequences. For instance, one respondent stated that: *'Health information should remain between doctor and patient and should not be shared outside the hospital. They (the medics) have the access to patients' data, and they can share my information with others without my consent or any alerts from the app'*. According to the results, the vast majority of our respondents (95%) are concerned about the security of their health-critical data. Just 1% (Figure 1) were less worried about health-critical data related to exercise and health tracking. (Bakheet et al, 2021).

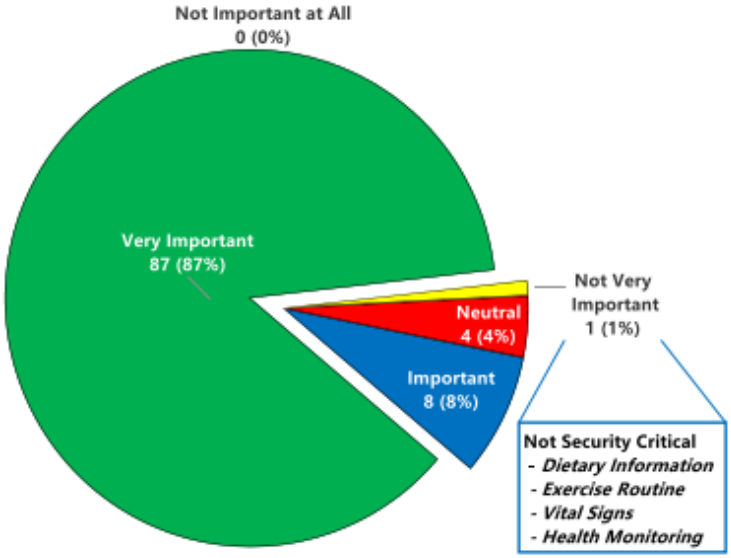

Figure 1: (Bakheet et al, 2021).

4. RESULTS, DISCUSSION, AND CONCLUSION:

After reviewing the literature and researching about the topic I would like to conclude with following finds with respect to hypothesis made:

Results, Discussion, and Conclusion for R1:

H1: There is one unified way of assessing privacy and security concerns of mHealth applications.

Hypothesis 1 has mixed results. A deep dive into a sample of existing literature shows conflicting themes emerge. Although a lot of different methods of assessing the privacy and security of mHealth applications is found, there has been a common theme of assessing the readability of privacy policy and conducting comparative analysis by developing a scoring model with various privacy and security measures.

The wide variety of mHealth applications make it easy for hackers to take advantage of and harm smartphone users, and a lack of regulation by FDA or other agencies gives developers the flexibility to upload their healthcare apps on the global market which poses a risk to the privacy and security of app users by providing them poorly developed features. The lack of a unified way of assessing privacy and security of these apps due to a large variety of apps and the lack of regulation prevents appropriately addressing the risks. Developing a taxonomy and categorizing the various mHealth applications on the dimensions of their privacy, security and intended usage can help us better understand the purpose of mHealth apps while also addressing the risks they have in common.

Results, Discussion, and Conclusion for R2:

H2: Data sharing by third parties is problematic and violates privacy.

Hypothesis 2 was accepted. Multiple research studies and literature reviews from the literature sampled in this study highlighted that aggregate data mining by third-parties can be linked back to the individual; one study concluded that 25% of research participants were correctly identified by name and 28% by address from data redacted beyond the HIPPA Safe Harbor standard. For instance, Medscape, an mHealth

app that provides medical information to clinicians and health professionals, uses Google's Firebase as a third-party storage; Firebase is a real-time data cloud storage network, and the use of third-party platforms to store data could increase the risk of data leakage (Zhao et al, 2020).

Results, Discussion, and Conclusion for R3:

H3a: Although applications have privacy policies, one of the reasons end users are not aware of privacy policies is because app developers do not make this information transparent.

Hypothesis 3a was accepted because one of the reasons why end-users are not aware of the privacy policies is the ambiguity with which they are written. The studies examined for this project indicate that health care privacy policies are written at a standard higher than understood and comprehended by the general population. This affects how easily an average individual can read and understand the privacy policies, making them unaware of what they are agreeing to when using the app. Hypothesis 3a is also accepted because a lack of transparency in privacy policies affect the users.

For example in a self tracking app study Over 40% of apps allow users to publish their activity to third-party services. Only 11% of apps, however, provide contextual privacy help, such as explaining the effect of sharing information with different audiences.

Application developers should simplify the privacy policies so they could be easily understood by the end-users. End-users need to have an improved and increased awareness of the many types of personal data that is collected and the privacy policy needs to be clear on dealing with such data.

App providers can also provide some instructions to the users as to how to create strong passwords to manage app access permissions in addition to guiding the users on security specific features of the app, motivating and educating them to learn about usability, functionality and security of the application.

H3b : Although applications have privacy policies, end users are not concerned with them and do not seek out this information voluntarily.

Hypothesis 3b was rejected because multiple studies in this project's sample conducted surveys where respondents showed concern about data privacy and how their data was being shared and requesting notification in case their data was shared with third parties. The only time users were not concerned about data privacy was when the data collected and shared wasn't health critical data. Otherwise, users wanted to be notified when health critical data was being shared even with the providers and authorized health personnel.

This means that end-users of mHealth applications are taking greater interest in knowing how their health critical data is collected and used and this will be an opportunity for application developers to provide safeguards and transparency to the users who download and use their applications.

5. FUTURE SCOPE

The privacy issues of mobile applications need to be dealt with carefully as users may unwillingly and unknowingly share very sensitive private data. As a result, it's important that all stakeholders, from app developers to legal consultants for privacy policy development, are involved in the creation of mHealth apps from the start to ensure that they're fully compliant with data protection laws and consumer privacy. Personal data privacy regulations are extremely important, and they must be supported. Individuals may be protected by well-designed privacy policies that require consent for the collection, use, disclosure, or retention of sensitive personal and health information, and they may restrict the use of this extremely sensitive data by enabling users to alter and revoke previous consent.

More study is needed to look at the dimensions of the categories of mHealth apps, which can be broken down into different subcategories. This study is more focused on providing a high-level overview of the variety of assessments available for mHealth applications. Further study is needed to organize the vast number of mHealth apps available to use and investigate different venues to approach the problem by exploring ways to assess the various categories of apps and establish a correlation between the ranking of apps and perceived concern for each subcategory.

REFERENCES

Barboutov, K., Wallstedt, K., Torsner, J., Sveningsson, R., Sachs, J., et al. 2017. ***Ericsson mobility report***. <https://www.ericsson.com/en/mobility-report/reports. Ericsson>. viewed 14 March, 2021

Benjumea, J., Ropero, J., Rivera-Romero, O., Dorronzoro-Zubiete, E., & Carrasco, A. 2021. Assessment of the Fairness of Privacy Policies of Mobile Health Apps: Scale Development and Evaluation in Cancer Apps. ***JMIR Mhealth Uhealth.*** 7(4):3-15

Biswas KK, Hossain A, Chowdhury R, Andersen K, Sultana S, Shahidullah SM, Pearson E. 2017. Using mHealth to Support Postabortion Contraceptive Use: Results From a Feasibility Study in Urban Bangladesh. ***JMIR Form Res***1(1):2-7.

Boulos, M. N., Wheeler, S., Tavares, C., & Jones, R. (2011). How smartphones are changing the face of mobile and participatory healthcare: an overview, with example from eCAALYX. ***Biomedical engineering online***. <https://pubmed.ncbi.nlm.nih.gov/21466669/> viewed 14 March, 2021

Bucci S, Morris R, Berry K, Berry N, Haddock G, Barrowclough C, Lewis S. (2018). Edge D. Early Psychosis Service User Views on Digital Technology: Qualitative Analysis. ***JMIR Mental Health***, 5(4):10091.

Campbell JI, Aturinda I, Mwesigwa E, Burns B, Santorino D, Haberer JE, Bangsberg D, Holden R, Ware N, Siedner M. 2017. The Technology Acceptance Model for Resource-Limited Settings (TAM-RLS): A Novel Framework for Mobile Health Interventions Targeted to Low-Literacy End-Users in Resource-Limited Settings. ***AIDS Behav***, 21(11):29-40

Cheung C, Bietz MJ, Patrick K, Bloss CS. 2016. Privacy attitudes among early adopters of emerging health technologies. ***PLoS One***, 11(11):1-12.

Conn, J. 2013. ***No Longer a Novelty Medical Apps Are Increasingly Valuable to Clinicians and Patients***.

<https://www.modernhealthcare.com/article/20131214/MAGAZINE/312149983/no-longer-a-novelty-medical-apps-are-increasingly-valuable-to-clinicians-and-patients>. viewed 8 March 2021

Constantino, T. 2013. ***Ims Health Identifies Opportunities for Mobile Healthcare Apps to Drive Patient Engagement, Enhance Delivery of Care***. Parsippany, NJ, <https://www.businesswire.com/news/home/20131030005221/en> viewed 17 March 2021.

Data and Reports 2020. ***Mobile Health (MHealth) Market To Reach USD 311.98 Billion By 2027: Reports and Data***. GlobeNewswire News Room. New York, <www.globenewswire.com/news-release/2020/04/28/2023512/0/en/Mobile-Health-mHealth-Market-To-Reach-USD-311-98-Billion-By-2027-Reports-and-Data.html> viewed 8 March 2021.

de la Vega R, Miró J. 2014. mHealth: a strategic field without a solid scientific soul—a systematic review of pain-related apps. ***PLoS One***.9(7):2-9

Dehling T, Gao F, Schneider S, Sunyaev A.(2015). Exploring the far side of mobile health: Information security and privacy of mobile health apps on iOS and Android. ***JMIR Mhealth Uhealth***, 3(1):7-10

Dubay, W. 2004. ***Principles of Readability***. < www.impactinformation.com/>. viewed 5 April 2020

Faezipour, Misagh & Faezipour, Miad. 2020. Sustainable Smartphone-Based Healthcare Systems: A Systems Engineering Approach to Assess the Efficacy of Respiratory Monitoring Apps. ***Sustainability***, 12(12): 5061.

Felt, A.P., Finifter, M., Chin, E., Hanna, S., and Wagner, D. 2011.***A Survey of Mobile Malware in the Wild, in A Survey of Mobile Malware in the Wild***. Working paper number 3-14, University of California, Berkeley 3-14.

Giunti G, Guisado Fernández E, Dorronzoro Zubiete E, Rivera Romero O. 2018. Supply and demand in mhealth apps for persons with multiple sclerosis: systematic search in app stores and scoping literature review. ***JMIR Mhealth Uhealth***. 6(5): 6-10.

Huckvale K, Prieto JT, Tilney M, Benghozi P, Car J. 2015. Unaddressed privacy risks in accredited health and wellness apps: a cross-sectional systematic assessment. ***BMC Med***.13:214

Kim, J., Campbell, A. S., de Ávila, B. E., & Wang, J. 2019. Wearable biosensors for healthcare monitoring. ***Nature biotechnology***, 37(4), 389–406.

Knorr K., Aspinall D., Wolters M. 2015. On the Privacy, Security and Safety of Blood Pressure and Diabetes Apps. In. ***Federrath H, Gollmann D. ICT Systems Security and Privacy Protection. SEC 2015. IFIP Advances in Information and Communication Technology***, Switzerland: Springer Cham.

Llorens-Vernet P, Miró J. 2019. Standards for mobile health-related apps: systematic review and development of a guide. ***JMIR mHealth uHealth***. 8(3): 2-6

Lupton, D., & Jutel, A. 2015. 'It's like having a physician in your pocket!'A critical analysis of self-diagnosis smartphone apps. ***Social Science & Medicine***, 133: 128-135.

Leibenger D, Möllers F, Petrlic A, Petrlic R, Sorge C. 2016. Privacy Challenges in the Quantified Self Movement – An EU Perspective. ***Proc Priv Enhancing Technology***, (4):315-334.

Meier, R., 2012. ***Professional Android 4 Application Development***, New York: John Wiley & Sons.

Mense A, Steger S, Sulek M, Jukicsunaric D, Mészáros A. 2016. Analyzing privacy risks of mhealth applications. ***Stud Health Technol Inform***, 221:41-5.

mHealth Solutions Market. 2020. ***Market Research Firm. MarketsandMarkets™ INC***. <https://www.marketsandmarkets.com/PressReleases/mhealth-apps-and-solutions.asp>. viewed 16 March, 2021

Millenson, M. L., Baldwin, J. L., Zipperer, L. & Singh, H. 2017. Beyond Dr. google: the evidence about consumer-facing, digital tools for diagnosis. ***Diagnosis***, 5(3): 95–105.

Misra, S., Lewis, T.L., and Aungst, T.D., 2013. Medical Application Use and the Need for Further Research and Assessment for Clinical Practice: Creation and Integration of Standards for Best Practice to Alleviate Poor Application Design. ***JAMA Dermatology***, 149(6): 661-662.

Minen MT, Stieglitz EJ, Sciortino R, Torous J. 2018. Privacy Issues in Smartphone Applications: An Analysis of Headache/Migraine Applications. ***Headache***, 58(7):1014-27.

Ostherr K, Borodina S, Bracken RC, Lotterman C, Storer E, Williams B. 2017. Trust and privacy in the context of user-generated health data. ***Big Data Soc***, 4(1): page unlisted.

Papageorgiou A, Strigkos M, Politou E, Alepis E, Solanas A, Patsakis C. 2018. Security and Privacy Analysis of Mobile Health Applications: The Alarming State of Practice. ***IEEE Access***, 6:9390-403.

Parker L, Halter V, Karliychuk T, & Grundy Q. 2019. "How private is your mental health app data? An empirical study of mental health app privacy policies and practices," ***International Journal of Law and Psychiatry***, 64: 198- 204.

Patrick JR. How mHealth will spur consumer-led healthcare. ***Mhealth,*** 2015(1):14.

Petrizzo, D. & Popolo, P. S. 2020. Smartphone use in the clinical voice recording and acoustic analysis: a literature review. ***Journal of Voice***, 2020(7): pages unlisted.

Plachkinova M, Andres S, & Chatterjee S. 2015. A Taxonomy of mHealth apps - Security and privacy concerns. ***Annual Hawaii International Conference on System Sciences***, 3187-3196.

Research And Markets Ltd. 2017. ***Mobile Health (MHealth) App Market - Industry Trends, Opportunities and Forecasts to 2023***. <www.researchandmarkets.com/reports/4435917/mobile-health-mhealth-app-market-industry>. viewed 8 March 2021

Research2Guidance. 2017. ***325,000 mobile health apps available in 2017 – Android now the leading mHealth platform***. <http://research2guidance.com/325000-mobile-health-apps-available-in-2017/> viewed 8 March 2021

Ronen, K., Unger, J. A., Drake, A. L., Perrier, T., Akinyi, P., Osborn, L., Matemo, D., O'Malley, G., Kinuthia, J., & John-Stewart, G. 2018. SMS messaging to improve ART adherence: perspectives

of pregnant HIV-infected women in Kenya on HIV-related message content. ***AIDS care***, 30(4), 500–505.

Scott, R. & Mars, M. 2014. Telehealth in the developing world: current status and future prospects. Telehealth in the developing world: current status and future prospects. ***Smart Homecare Technology and Telehealth***, 2015(3): 25-37.

Segura Anaya LH, Alsadoon A, Costadopoulos N, Prasad PWC .2018. Ethical Implications of User Perceptions of Wearable Devices. ***Sci Eng Ethics***, 24(1):1-28.

Stawarz K, Preist C, Tallon D, Wiles N, Coyle D. 2018. User Experience of Cognitive Behavioral Therapy Apps for Depression: An Analysis of App Functionality and User Reviews. ***J Med Internet Res***,20(6):10120.

Visvanathan, A., Hamilton, A., and Brady, R. 2012. Smartphone Apps in Microbiology—Is Better Regulation Required?. ***Clinical Microbiology and Infection***, 18(7):218-220.

World Health Organization.2011. mHealth New horizons for health through mobile technologies. World Health Organization. https://www.who.int/goe/publications/goe_mhealth_web.pdf.

Zhao W, Shahriar H, Clincy V & Bhuiyan Z.A. 2020. Security and Privacy Analysis of Mhealth Application: A Case Study. ***2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)***, Guangzhou, China,1882-1887

Zhao Y, Zhu X, Perez AE, Zhang W, Shi A, Zhang Z, Gao P., Wang J., Yang C., Zaller N., Sun Y., Operario D., Zhang H. (2018). MHealth approach to promote oral HIV self-testing among men who have sex with men in China: a qualitative description. ***BMC Public Health***,18(1):1146.

Zhou L, Bao J, Watzlaf V, Parmanto B. 2019. Barriers to and facilitators of the use of mobile health apps from a security perspective: mixed-methods study. ***JMIR Mhealth Uhealth***.7(4):2