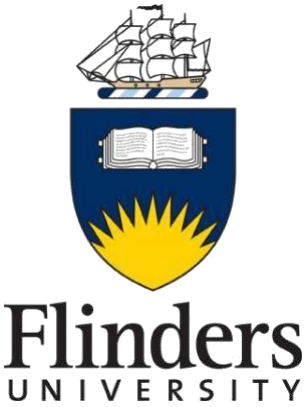

Mobile Health App Privacy Assessment

Submitted by: Jasmeen Chahal

Student id: 2187269

Supervised by:

Professor Trish Williams

November, 2019

Thesis submitted to the College of Science and Engineering in partial fulfilment of the requirements for the degree of Master of Science (Computer Science) at Flinders University, Adelaide, Australia

Declaration

I certify that this thesis does not incorporate without acknowledgment any material previously submitted for a degree or diploma in any university. To the best of my knowledge and belief it does not contain any material previously published or written by another person except where due reference is made in the text.

Jasmeen Chahal

(8th November, 2019)

Acknowledgements

I would like to thanks Brett Wilkinson who provided me an opportunity to work on this study. I am sincerely grateful to Professor Trish Williams for her guidance and valuable feedback throughout the duration of my study. Her valuable suggestion helped a lot to complete this work. I am also thankful to Gihan Gunasekara for his support to improve my work. I would also thanks to all staff members of the College of Computer Science and Engineering at Flinders University for their support provided to me along the way, and thanks to authors whose studies helped me in the completion of this study.

At last but not least, many thanks to my family and friends who supported me a lot during my studies with their care and love. My work could not have been possible to complete without their support and encouragement.

Abstract

Mobile applications such as healthcare apps have become an essential part of people's lives. Increasing growth of mobile apps create both opportunities and challenges. Information privacy in mobile apps is becoming increasingly critical. Users experience privacy concerns in apps information permission sensitivity and sharing of sensitive, personal user data by apps with third parties. To protect users against possible privacy risks, some mobile app advertisers prominently disclose app permission requests on app download pages. However, there is no opt-out facility for customers if they wish to download and use the app on their mobile device. Privacy concerns in health apps are involved with user's personal and medical information that might be encoded by third parties or become vulnerable to attack by cybercriminals. Despite the problematic nature of this issue, there has been little research focused on the assessment of mobile apps privacy. Focusing on this emerging practice of assessment, the aim of this study was to evaluate the privacy of mobile apps. Using a mixed studies review method, the study investigated the privacy assessment of mobile apps, especially in the health and wellness area. It found that there are increasing concerns for safety of health app users and an urgent need for the development of app privacy assessment tools for consumers. The results of the research provide a better understanding for the mobile app developers and users to recognize the importance of protecting the privacy and security of users.

Table of Contents

CHAPTER 1: INTRODUCTION

1.1 Overview

Smart phones and handheld personal computers have become crucial for organizations and people in the 21st century information society, where creation, dissemination, and sharing of information is increasingly dependent on digital devices connected to the internet. Statistics show that in 2019 around 3.5 billion people, or almost half of the world's population, use the internet at least once a month or go online through mobile devices or laptop/desktop systems (Kemp, 2019). According to e-Marketer updates and prediction (Editors, 2017), for the period 2017-2021, this level of internet use will increase from 3.46 billion to 4.14 billion, and there is a probability that 84.7% will use smart phones to access the internet. Android phones are more popular than Apple according to a 2018 Q2 market share analysis (Framingham, 2018). These devices provide the functionality in the form of mobile applications, commonly referred to as apps, which are software programs designed to run on a mobile device, such as a phone, tablet, or watch.

Many applications, for example, e-shopping or internet banking, provide the features that are essential for the daily business or personal activities of people. These handheld devices or smart phones have features, such as Wi-Fi (Wireless Fidelity), Bluetooth, GPS (Global Positioning System) and NFC (Near Field Communication), which enable a wide range of connectivity. In addition to internet connectivity, these phones also have capacity for storage and sending of personal information, including email, messaging, contacts, videos, photos, social networking, and banking credentials. Accessing personal banking details of internet users is particularly attractive to malware developers who target vulnerable devices with viruses that allow them to gain electronic entry to bank accounts and withdraw funds.
Many mobile apps access the smart phone resources and distribute user data after consuming the data, which may lead to privacy issues and vulnerability of the device to viruses. According to Google and other internet reports, the number of malware viruses is increasing by up to 165% each year (Framingham, 2018). The growth in demand for mobile apps is also increasing rapidly and, consequently, there is a need for a secure development process for apps, which protects the user's device from cyber-criminals and ensures protection of privacy.

In addition to the threats from malware viruses attacking a user's device, it has been revealed that some apps are sharing users' data with others for commercial purposes through referral partnership contracts. In the case of health apps, it has been found that some are sharing private medical information of users without their knowledge or permission (Grundy, et al., 2019). One recent study found that 80% of health apps presented privacy issues for users. For

example, some health apps share user data for improving knowledge and research about health issues; however, there is lack of transparency about the practice and some apps do not obey the HIPAA (Health Insurance Portability and Accountability Act) rules, which require a baseline of privacy protections appropriate to sensitive medical data. Therefore, mobile privacy assessment tools and techniques are needed on smart phones, which can reduce the privacy risk and provide protection against cyber-crime and other types of threats, which exist in the online environment.

1.2 Problem statement

A mobile device handles diverse types of user data. For example, it stores contacts, emails, and important notes. Mobile apps are software applications that are designed to run on mobile devices. There is a multitude of statistical information about the spread and use cases of modern technology. Google Play Store and Apple's App Store are two main app stores in the world. As per of the research of March 2017, Google Play Store and Apple's App Store had 2.8 million and 2.2 million apps, respectively (Medium, 2019). These apps require users to agree to terms of service before they are permitted to download and access the software features. There are no opt-out facilities for any applicant who does not want to accept the conditions; they are simply precluded from using the app.

However, studies have shown that most mobile app users neglect to study or even read the important information when they complete their agreement with privacy details of software, for example, privacy policies, and terms of service. Mylonas et al. (2013) asserts that many android mobile users ignore the permissions or notification, or sometimes cannot understand the permissions. In addition, users may not even notice that the less useful app on their mobile knows more about them than it should. For example, a mobile application could track the user's location and access contact details, monitoring online habits and jeopardizing privacy of the user. These security and privacy problems with apps exist in many areas of digital communication; however, in health apps the problems have been found to be particularly prevalent and pose a serious risk to the health and welfare of users.

According to a report in the HIPAA Journal (2019), 31.6 million healthcare records were breached by mHealth app, between January 2019 and June 2019, which is double all of 2018. Moreover, the increase in health wellness apps raises privacy concerns. There are a number of mobile apps that target applications in the health and medical sector. Such apps can track the diet plans, steps, sleep, set reminders to take medicines, and those that assist people to get involved in self-help communities with people with similar ailments. To work properly, the software needs access to user information. If this information is spread or misused, however,

the same information can cause harm to the user's life, situation, and reputation. The three technical causes of privacy risks in mobile health and wellness apps are unencrypted data, embedded advertisements, and third-party analytics services. These three causes can create the top four privacy risks of mobile health apps:

- Collecting passwords
- Collecting banking details
- Collecting disease symptoms
- Collecting disease status (Sampat, & Prabhakar, 2017).

1.3 Research questions

This study examined the following questions in order to assess mobile app privacy:

1. How do mobile apps for health handle privacy and can the level of privacy be assessed?
2. What would a mobile app privacy assessment tool for consumers look like?

To answer these research questions, a mixed studies literature review method was conducted. The methodology communicates through a descriptive scenario and overall detailed description of mobile health & fitness apps, which are evaluated to assess the level of privacy to help potential app users to decide for themselves if the app is safe and without privacy issues.

1.4 Research Purpose

Health information is considered sensitive information. The aim of this research study was to analyse the popular mHealth apps from the Google Play Store and iOS App Store to assess the privacy. The study conducted an analysis of the legal documents which are to accompany software products which use personal user data. The study investigated the privacy issues, data privacy, and policies associated with health and wellbeing mobile apps. The research study focused on the privacy assessment of mobile applications to ensure user sensitive data protection is present to protect against different attacks and malicious activity and thus reduce the privacy risks. Mobile applications represent new privacy concerns because they are downloaded to a personal device where most users store their personal information more than they would on a laptop or other devices.

This research is significant as it will be helpful to identify the default app privacy setting which is based on a user's preferences for different apps. Therefore, a user will be able to select the default setting when configuring mobile app privacy settings. This way a user

could reduce the burden of other privacy settings, which requires user's preferences for apps.

1.5 Structure of the thesis

The structure of this thesis is, firstly, to provide the background of the problems related to the mobile health apps and privacy concerns in them. There follows a discussion of the review of the body of literature related to mobile app privacy in healthcare and linkages to this present study. Next, is a description of the methodology, followed by a discussion of the results obtained from the study. After that, steps involved to conduct the research method are defined. Finally, the conclusion is presented.

CHAPTER 2: LITERATURE REVIEW

2.1. Overview

A literature review is an essential part of a research study to analyse previous research in this area and identify the gaps in this research (Ridley, D. 2012). In this part, relevant information about the research issue is collected from published sources, such as books, academic journals, articles, and reliable websites. A literature review provides an opportunity to the researcher to collect appropriate information about the research issue from a wide range of data sources, which can be used to further the research objectives.

In this study, the literature review discusses related research studies in the area of assessing mobile app privacy and explains how these studies have informed the premises for the assessment of privacy in mobile apps. The discussion will identify the gaps in the research and indicate the contribution the current study can make to the body of knowledge on the subject.

The objective of this research is divided in three main sections: first, a systematic literature review of the factors that are influencing effective use of mobile health apps for data privacy, second, identify the most common issues of mobile apps and, third, the results of previous existing studies in relation to the assessment of the privacy of mobile health apps. A brief overview of the studies related to the work is used to create an understanding of the present state of technology and the threats.

Huckvale, et al. (2012), discussed the adapted systematic review methodology for the assessment of apps. They identified English language health apps (asthma) for all ages through a systematic search. The research found that 89% (n= 70/79) of applications were transmitting data to internet facilities. No personal data encrypted app stored locally. In addition, 66% (23/35) of applications send identifying information which did not use encryption and 20% (7/35) of apps did not have a privacy policy. Overall, some form of privacy policy was used by 67% (53/79) of apps. No application gathered or transferred data that it would not be clearly indicated by a strategy; however, 78% (38/49) of data transmitting applications with a strategy that did not portray the type of private data were included in applications. Without encoding, four applications sent identification and safety data (Huckvale et al, 2015). To participate in the research, people used an Android app for this examination. Of those, 16% of participants were able to install the application and, over 90% participants were in agreement with some portion of the extensive data collection (Huckvale et al, 2015).

Moreover, the authors found that there was a systematic gap in accredited health applications compliance with data protection principles, which led to a question of whether certification programs that rely heavily on developer disclosures can provide patients and

clinicians with a trusted resource. Accreditation programs should provide reliable warnings or at least be consistent about potential issues and require an app developer disclosure that provides reliable resources to users (Huckvale et al, 2015).

Sunyaev, (2014), assessed mHealth apps for the scope of privacy policies and what information is offered. That study surveyed the most rated, English language mHealth apps in the Google Play Store and Apple iTunes Store. In another study, many concerns are discussed in their study relating to privacy of health apps that were aimed at the consumers or healthcare providers, and whether they should be controlled and assessed by the US Food and Drug Administration (FDA), (Maged N. Kamel Boulos, 2014). Nicholas et al. (2015) identified the apps for Bipolar Disorder in the iOS and Google Play stores to assess their features and the quality. They applied a systematic review framework for the search, screening, and assessment of apps.

2.2. Health application

A health app is application software that is related to health services for mobile phones and PCs. Health apps help users to learn about their health and can be a great step towards being a healthier individual (McLachlan, 2018). There are a number of mobile health apps available from app stores that assist people to improve health and to achieve goals. Examples are CalmHealth, HealthEngine, Pacer, Runkeeper, and Strava (McLachlan, 2018).

Figure 1 has been removed due to copyright restrictions.

According to Figure 1, over the next five years, the Asia Pacific Region is expected to have the world's highest growth rate in the mHealth market from 2019 to 2024 (Intelligence, 2019). In North America and Europe, there will also be gradual adoption of mHealth services, which will be followed more slowly by Africa and the Middle East (Intelligence, 2019). By 2025, much of the world's population is expected to have access to mHealth app programs direct to their mobile devices and to have the benefit of information interventions that automatically transmit health advice to selected communities. These mHealth applications have already begun to improve the connectivity of individuals with health agencies and professionals to be updated about the latest healthcare issues, such as nutrition, medicines, and medical treatment, in a most efficient manner. App users can connect with health professionals with increasing degrees of self-examination and health assessment, including monitoring blood pressure, cardiac health, diabetes, respiration, and other vital indicators. The app is particularly important for remote communities and people living or travelling some distance from doctors, specialist healthcare professionals, and hospitals, as they can consult their app for specific health advice.

It is stated by McLachlan (2018) that healthcare applications have also become advantageous for the nurses, doctors, and associated medical staff in the care services. Health applications are helpful for the doctors to monitor the health condition of their patients and provide regular guidance, for example on diet and fitness, without the need for an appointment. Approximately, 93% of doctors believe that the health applications are able to bring improvements in the health of their patients. Indeed, there are doctors who are already using mobile technology to deliver quick care services for their patients (Kounelis, 2012). According to Kounelis (2012), as access to the Internet and smart phones have reached every corner of the world, individuals can acquire essential information about healthcare easily and can get the healthcare benefits without a physical consultation with healthcare professionals or using tele consultations.

Therefore, it is clear that mobile apps for health and wellbeing are becoming increasingly popular and beneficial; however, there is little research on assessing mobile apps for privacy. Security and privacy are also critical issues in society, where hacking, cybercrime, online scams, and identity theft are increasingly prominent social problems. Improving information privacy in mobile apps for health and wellbeing is a serious concept. Lack of security and privacy in mobile applications can compromise the important services of health systems. The highest risk is associated with the data that represents the vulnerability of privacy and can be misused for a fraud, for example, passwords and banking details. Sometimes the location of a user, which can be very sensitive data, is important because if any adversary intercepts the user location, the attributes of the user and their social relations are also traced by the adversary or any attacker. Therefore, mobile privacy assessment tools and techniques are essential for individuals on smart phones to reduce privacy risk and provide protection against any type of risks.

2.3. Personal information

The Office of the Australian Information Commissioner (OAIC, 2014) states that "Personal information is information that could identify an individual, or an individual who is reasonably identifiable". The Australian Privacy Act applies to Australian government agencies, all small and large businesses, all private health services, the credit reporting industry, and all organisations trading in personal information (OAIC, 2019). Data privacy focuses on the use and governance of personal data, including putting policies in place to ensure that consumers' personal information is being collected, shared, and used in appropriate ways (Hughes, 2019).

Mobile privacy refers to information or data shared with mobile applications, how that data is used, and who that data is shared with.

2.4. Privacy in health applications

Mobile technology has many advantages for providing actionable medical advice; nevertheless, it also has limitations and potential problems associated with it. Privacy is one of the major concerns (Maged N. Kamel Boulos, 2014). Privacy is the right of an individual which defines what information or data they would like to share with others, who is permitted to know that information, and the ability to determine when others can access that information (Bizannes, 2007). In other words, privacy is the right of freedom from intrusion or interference. Information privacy is the right to have control over your personal information, as well as how it is collected and used (Hughes, 2019). In Australia, the Commonwealth Privacy Act protects the personal information (OAIC, 2014).

There are many concerns related to safety of health apps aimed at the general public or healthcare professionals, and whether they should be assessed and controlled by the US Food and Drug Administration (FDA) (Maged N. Kamel Boulos, 2014). These authors present many technologies and aspects related to mobile app privacy assessments. Habib et al. (2018) discussed the Trust4app. This app ensures that the entire downloaded app from Play Store is malware free or does not contain fake data, such as reviews and ratings. A trust score is calculated which determines whether the app is trustworthy or not. Zhao et al., (2018) presented the location privacy systems in social apps, stating that either the app is susceptible to the location inference attack or not. Hamed et al., (2018) presents a privacy-scoring model that assesses the risk to user privacy based on permissions set. The constraints of this model are the relative importance of permissions and severity and their interactions. The authors tested a set of 64 applications by defining association rules using data mining. Rosenfeld, Torous, & Vahia (2017) presents an analysis of existing privacy policies of different apps, and they identify how dementia apps protect the user data and which privacy policies this app has.

A number of studies have discovered that many android users ignore the permissions or notification or sometimes cannot understand the permissions (Apostolopoulos, 2013; Alexios Mylonas, 2013). Therefore, by agreeing to the conditions and policies, they expose themselves to the risk of loss of privacy of their data or personal information. Any information that is shared with an application or gadget could be imparted to any number of outsiders without the knowledge or approval of the user. A security explanation may help a person considering an

application to decide how unsafe it is, and to evaluate the risks of sharing their information the application or gadget. Undoubtedly, mobile phones, tablets, and wearable devices such as smart watches have made communication and access to information much easier. Regardless of their numerous advantages, however, portable gadgets, applications, and wearables are profoundly security intrusive, gathering information about the user, which may routinely be made available to third parties (Clearinghouse, 2013).

According to the findings of a joint study by Penn State University and Duke University researchers (Enck et al., 2010; Enck et al., 2014; Penn State, 2010), many mobile apps transmit the users' unique identifier and location to third parties, such as advertising services, and some shared details of gender, age, location, phone number, SIM card serial number, and other sensitive, personal data. Advertising networks and analytic services pay for the information, which is often used for ad-targeting purposes, however, could also be used by cybercriminals to target users.

Health and wellbeing applications, in particular, gather a considerable amount of individual data necessary to enable user-specific health consultation and advice. Applications may require clients to enter their name, email address, age, sex, height, weight, and a photograph. Versatile applications (different types of applications), particularly applications that are being downloaded for free, rely upon promoting, advertising, and partnering arrangements to maintain profitability. Consequently, they may share recognisable user data with sponsors, or permit advertising systems to follow the users' online activity.

According to a recent report by ABC News (2019), Australia's top healthcare appointment booking application, HealthEngine, is facing a fine of millions of dollars due to selling their patient data. The ABC investigation of HealthEngine revealed that it was sharing patients' personal data, such as their names, email addresses, phone numbers, and other details to law firms (McGrath, 2019). Yet, the privacy policy of HealthEngine states that they may disclose a user's personal data to third party providers, such as software service providers or their professional advisers or lawyers, but only for the purpose of providing services to users. Thus, their actions have been shown to contradict the stated claims concerning privacy guarantees for users. As a result of the investigation, the Australian Competition and Consumer Commission (ACCC) chairman, Rod Sims, said, "Patients were misled into thinking their information would stay with HealthEngine app but, instead, their information was sold off to insurance brokers" (McGrath, 2019). HealthEngine app is also under investigation for misleading users by manipulating users' reviews of medical practices (McGrath, 2019).

2.5. Issues about app privacy

Table 1 illustrates the common privacy and security issues of mobile apps with reference to apps in which these issues have occurred.

Table 1. Occurrences of privacy breaches of mobile apps

Issue	Description	Reference
1. Data leakage	Data leakage is caused due to issues negligence of security in the framework which is not in control of the app developer (Mugge, 2014).	In May 2014, there was a one of major data leakages was of personal information of 145 million eBay customers, such as names and emails addresses, by which millions of customers were affected (Wakefield, 2014).
		Another incident happened in 2016. In this incident, two hackers hacked the personal details of 57 million Uber users and exposed six million drivers' license numbers (Armerding, 2018).
		In 2015, the largest data breach in healthcare was discovered. It was noticed by a database administrator of an Anthem associate that a database query was running by using admin login data. In this incident, attackers obtained personal data of their members as well as medical information. This breach impacted all the lines of Anthem, such as Unicare and Healthlink (Ragan, 2015; Armerding, 2018).

		Such incidents may cause damage to the reputation of organisations as well as financial loss.
2. Weak Server Side Controls	Any communication, which occurs between the app and the consumer outside the mobile phone, occurs via a server. In this manner, a weakness in security can be exploited by hackers. The serious threat emerges when app developers do not embrace traditional server side security contemplations under the account, due to lack of knowledge or small security budgets (Mugge, 2014)	According to security researcher, the Viper smart start app has a failure of authorising users. When a user logs in to the server then it changes the identification of the vehicle and get access to information, such as car location (Krisiina, n.d.).
3. Poor Authorization and Authentication	Poor or missing authentication allows unauthorized user or organisation to access data or backend server of the mobile app. Mobile device connections are not trustworthy. Mobile apps can require offline authentication to maintain the uptime. This offline requirement can create security loopholes. These should be considered by app developers when implementing the mobile authentication (Mugge, 2014).	Most common problem of authentication is faced in Grab Android app in 2017. Grab is a ride hailing application commonly used in Southeast Asia. It had an issue with Two-factor authentication, which could be helpful for an unauthorized organisation to gain access to user's account with the information of ride and payment by bypass 2FA authentication on Grab app (Krisiina, n.d.).
4. Broken cryptography	Broken cryptography happens because of incorrect implementation, bad encryption, or use of insecure algorithms. (Mugge, 2014).	Major issue of cryptography is discovered in the Ola app. It has weak AES/ECB/PKCS5Padding cryptographic keys to encrypt passwords. It also has issues related to insufficient transport layer and protection (Krisiina, n.d.).
5. Improper session handling	Improper session handling is the continuance of the previous session for a long time period even when the user is switched from the app (Mugge, 2014). Any other person who gains access to the device can take control over the app and steal data or modify the important data (Mugge, 2014).	Most common ride hailing app Grab has issues of weak session management and failure to maintain security of user's identity (Krisiina, n.d.).

2.6. Data stages

In mobile apps, data is categorised into three stages as shown in Figure 2:

Figure 2 has been removed due to copyright restrictions.

a. Data in use: Data in use means data that is utilised by an app or a user (Sealpath, 2014).

b. Data in transit: Data in transit means data that transfers via messages, emails or other communication channels (Sealpath, 2014.).

c. Data at rest: Data in rest means data that stored in database or a drive (Sealpath, 2014).

The risk for data in use, rest, and transit depends on the privacy measures of apps. Encryption is a most effective method to protect data. The best data protection practices for data in rest and transit are as follows:

- Users should apply network security solutions, such as network access control and firewall. This will help to secure the networks that are used to transfer data against intrusions.
- Users should apply data protection solutions with policies which will automatically encrypt the most sensitive data in transit or enable blocking, such as when a user wants to transfer an email with attached files or move to cloud storage (Sealpath, 2014).

If a user uses a public, private, or hybrid cloud to store data then there is a need to evaluate cloud vendors based on security measures (Sealpath, 2014).

2.7. Principles of data protection

The principles of data protection in mobile apps are as follows:

1. Storage limitation: Personal data or information ought to be stored in a structure which permits recognizable proof of information subjects for no longer than is fundamental for the reasons for which the individual information is handled.

2. Integrity and confidentiality: Personal information ought to be prepared in a way which surety the privacy of the user data, including insurance from unapproved get to and against information harm, misfortune, using appropriate technical measures.

3. Accuracy: Personal information ought to be exact and steady structure.

4. Data minimisation: Personal information ought to be sufficient and restricted to what is vital in connection to the reasons for which it is handled.

5. Lawfulness, fairness and transparency: Personal information ought to be legitimately, decently and straightforward in connection to information subject (Kearns, 2017).

2.8. Current ways to measure privacy in apps

To protect privacy, it is required to identify the ways in which a mobile app handles personal data. An investigation may include having to change the way mobile app stores personal data. Those ways are as follows:

2.8.1. Privacy by design

A privacy by design (PBD) approach should be adopted by a mobile app developer, a business, or government department. This approach promotes protection and data privacy built into the design specifications and design of information and communication systems to encourage compliance with privacy and information standards (OAIC, 2014). The Information Commissioner's Office (ICO) encourages organisations to consider privacy and data protection throughout a project lifecycle that includes collection, use, disclosure, storage, and destruction of data (OAIC, 2014). Implementation of a PBD approach will help developers to make sure the apps are privacy-friendly, whether or not their business is covered by the Privacy Act (OAIC, 2014). There are indications that some users, particularly the newer generations of internet savvy young people, are becoming aware of online privacy issues and are adopting safer practices. For example, a survey in 2013 by Pew Research Centre, found that 51% of youngsters had avoided certain apps over privacy concerns, and 26% had uninstalled an app because it was collecting personal information that they did not wish to share (OAIC, 2014).

2.8.2. Laws and Regulations

The laws and regulations define the formal requirements, which a manufacturer must provide concerning user privacy and security. Privacy laws are different across the world. There are a number of groups that provide guidance on laws and regulations affecting privacy. These include governmental and non-governmental organisations, which can publish standards and recommendations that augment the legal baseline. Certification is a scheme aiming to facilitate transparency for consumers. An app developer is responsible for compliance with laws.

- **APP (Australian Privacy Principles)**

The Privacy Act 1988, is the main legal framework which includes Australian privacy

principles (APPs)and is the principal legislation governing the privacy of information and protection of data. This act developed 13 Australian Privacy Principles (APPs) for the management of information (Raul, 2017). The Office of the Australian Information Commissioner is charged with responsibility for the Privacy Act (Raul, 2017). The OAIC is responsible for the policies for the protection of the private or personal data of the users and their sensitive information. As per the Privacy Act, the app manufacturers or organisations are not legally authorised to use and collect sensitive data of the users without the consent of the users (Jaikobs, 2014).

The 13 APPs for mobile app development are (Dempsey, 2014; Raul, 2017):

1. Open and transparency of personal information (APP1)
2. Pseudonymity and anonymity (APP2)
3. Solicited personal information collection (APP3)
4. Collection of unsolicited personal information (APP4)
5. Notification of personal information collection (APP5)
6. Disclosure or use of personal information (APP6)
7. Direct marketing (APP7)
8. Disclosure of the cross-border personal information (APP8)
9. Adoption, disclosure, or the use of public-related identifiers (APP9)
10. Quality of personal information (APP10)
11. Personal information security (APP11)
12. Access to personal information (APP12)
13. Correction of personal information (APP13)

- **GDPR (General Data Protection Regulation)**

The European Union's (EU) new General Data Protection Regulation (GDPR) has a risk based approach for privacy rules which focuses on protecting the personal data of individuals in apps. The GDPR is a regulation in EU law on data protection and privacy for all individuals within the European Union and the European Economic Area. The GDPR applies to any

company doing business with people in the EU. This regulation alters how business and public sector organisations can handle the data of their customers. Also, this law gives rights to individuals to have more control over their information (iapp, 2017). In the United States, personal data is regulated by the sector of personal information, such as health or financial sectors, and the methods data are collected, such as online or physically (iapp, 2017). The following are types of privacy data that GDPR protects (Nadeau, 2018):

- Basic identity information, such as name and address
- Web data, such as location or IP address.
- Political opinion
- Health and genetic data
- Biometric data
- Sexual orientation
- Racial or ethnic data

- **HIPAA (Health Insurance Portability and Accountability Act of 1996)**

The HIPAA is United States legislation that provides data privacy and security provisions for safeguarding medical information. It contains the following three major provisions:

- Portability
- Medicaid Integrity Program/Fraud and Abuse
- Administrative Simplification

Privacy of health information, security of electronic records, administrative simplification, and insurance portability are four main purposes of HIPAA. Health data is safeguarded to prevent it from being accessed by unauthorised individuals, and HIPAA protects the privacy of patients by prohibiting certain uses and disclosures of health information. The Act applies to health plans, Health Care Clearinghouses, and those health care providers that conduct health care exchanges electronically (Services, 2003).

A number of researchers have argued that mHealth applications have so far failed to align with the privacy protections guaranteed by the HIPAA (He, Naveed, Gunter & Nahrstedt, 2014).

2.9. Summary

Health applications play an essential role in keeping patient's data in a proper manner that is used by the care providers to evaluate the history of patient care. However, the privacy concern has influenced the reliability of health application technology in the healthcare sector. The major privacy issue with health applications is the safety of personal information of the patients. The technological advancement has generated the problem of hacking personal information of the individuals during online access of the healthcare services. Several fake applications are stealing personal data of individuals and fraudulently obtaining benefit from the patients through online access to healthcare services. To overcome this concern, the individuals should protect their devices through appropriate antivirus software and authorised access; however, the apps themselves may be subject to intrusion and may also be sharing patient data with others without the knowledge or agreement of patients.

An analysis of the literature review has revealed important information about mobile app privacy and some serious concerns about the inadequacies and practices of some app developers. This study investigated the level of privacy in mobile apps, which can be assessed and methods of privacy management used by health apps. As a part of this research, the study explored the research techniques to find the answers to these privacy problems and concerns. The findings of this study may be important to improve understanding about the privacy concerns in the digital healthcare system and determine the most suitable mobile app privacy assessment tools for consumers.

CHAPTER 3: METHODOLOGY

The research methodology chapter explains research techniques that are used for an analysis. In a research study, the methodology chapter is developed to find the appropriate solution related to the research issue. The term “Research Methodology” is considered as a foremost part of a research study to collect and analyse the research information for effective decision-making (Alvesson & Skoldberg, 2017). It is a theoretical and systematic method to conduct a research study. This section also develops understanding about the nature of the research issue. It is an essential part of the research in which the researcher collects the information through research approaches, data collection methods, and strategies (Robson, 2011). The research methods and approaches that are selected support the achievement of the research aims and objective. The selection of different approaches used during the methodology is effective to gain the in-depth knowledge or understanding of related problems or issues associated with the research project (Silverman, 2016). It is helpful in planning the entire research work in the most efficient manner and defining the significant structure to conduct the research in an effective manner using the most appropriate approaches for the research.

The aim of this research methodology is to illustrate the method that answers the two research questions: How do mobile apps for health handle privacy and can the level of privacy be assessed? and, what would a mobile app privacy assessment tool for consumers look like? Accordingly, this study determines whether the level of privacy in mobile health apps can be assessed. Additionally, this research investigates the app privacy assessment tool for consumers.

As a research methodology, the study uses a mixed method of inductive and deductive approaches towards finding the answers to the research questions through a review of the body of published literature on the topic of mobile health applications and their privacy concerns. The inductive research approach is often used in health and social science research and evaluation and is a flexible way to search towards the conclusion, as it does not involve any theory or hypothesis formed at the beginning of the research. Hence, the inductive method avoids any assumptions or predictions that could alter the direction of the research.

3.1. Research Design

Research design characterises a plan for the investigation of the research problem (Melnikovas, 2018). The research methodology is based on the theoretical concept of the Research Onion (Melnikovas, 2018). The Research Onion provides a description of steps to formulate an effective methodology, which defines the usage of qualitative and quantitative methods (Melnikovas, 2018). Figure 3 represents the stages of the Research Onion model.

Figure 3 has been removed due to copyright restrictions.

3.2. Research Philosophy

Philosophy is the first layer of the Research Onion which includes positivism, realism, interpretivism, and pragmatism. This provides guidance to gather and analyse the information for research. A pragmatism view helps a researcher to judge a topic from the constructive and objective views. The interpretivism view helps a researcher in interpreting the performance of people in the aspects of cultural and social life. The realism view is about continuous research. With the view of positivism, a researcher can find the explanations to test the accepted knowledge of the world, such as the law of gravity (Melnikovas, 2018).

3.3. Research Approach

The second layer of the Research Onion is a research approach that is considered as an essential component of the research methodology section to develop in-depth understanding about the research issues. An appropriate research approach facilitates a meaningful presentation of the research findings in a logical and systematic manner. The positivist view of research approach considers the existing research studies that are presented by other researchers, in the case of this study, by exploring information regarding mobile health apps and architecture in the area of information privacy. This helps to discover the reliability and privacy of user's data in apps that are used in the healthcare system. In this model, there are two types of research approaches: inductive research approach and deductive research approach (Melnikovas, 2018). These research approaches can be used to present the research findings in a systematic manner; however, the two research approaches are dissimilar to each other in terms of their nature (Alvesson & Skoldberg, 2017). This study examined the existing literature in the area of mobile app privacy assessment. In this study quantitative approach is conducted by gathering data from different sources, such as research reports, journals, and scholarly articles, for the assessment of privacy in apps. Qualitative approach of this study defines the impact of data collected from different sources.

The inductive research approach is correlated with the implementation of new ideas that come into view from the collected data, while the deductive research approach is incorporated with the use of theories through which the data may be collected and tested. The inductive approach is generally focused to gather the information from different sources in order to make detailed observations for that information and using that detailed information. Abstractions are made from this information based on different aspects and how data relates to the aims of the research (Melnikovas, 2018).

In this study, the inductive research approach helps in identifying the different ways to develop privacy assessment methods for mobile app privacy. This method is used because of its effectiveness for collection of qualitative data from different sources in order to make detailed observations of the information. On the other hand, the deductive approach can be used for analysing the privacy concerns of mobile health applications. Inductive approaches help in interpretation of views and opinions of different researchers. In addition, the inductive research approach is effective in interpreting views and opinions of different persons about the privacy concerns in health applications (Kumar, 2019).

In mixed studies, qualitative research is mainly associated with inductive methods, while quantitative research is most frequently connected with deductive methods (Melnikovas, 2018). Therefore, this research uses mixed methods - inductive and deductive - for the study and analyses of information from review of resources in the body of literature on health applications. Quantitative research in this study includes the number of reviewed articles in this study, whereas qualitative research defines the impact of reviewed studies on this research study.

3.4. Research Strategy

In the Research Onion, research strategy includes experiment, survey, case study, action research, grounded theory, archival research, and ethnography of research. Research strategy helps the researcher to select data collection methods to solve the research issues (Melnikovas, 2018). This study follows the archival research strategy, which allows the exploration of archived documents and existing information related to research study.

3.5. Research Methodological Choice

The research methodological choice is the fourth layer of the Research Onion model, which demonstrates the research method. As this study used a mixed methods approach, which included both quantitate and qualitative studies, analysis was used to examine the privacy in apps. In this study, the research studied the previous literature based on mobile app privacy assessment. Information is collected from previous studies including research articles, journal articles, books and conference papers to assess privacy in mobile apps. This method is used to understand the area of concern, to know what is already studied in this area and to identify the gaps in knowledge in the literature.

3.5.1. Review design

This research is conducted by mixed study review. According to Oliver et al. (2005), "Reviews are helpful in decision making about effective interventions to implement in each of the topic areas as well as decisions about the future development and evaluation of interventions" (Oliver et al., 2005, p. 430). A literature review is a significant component of mixed studies review that provides the background information to identify the level of privacy assessment of healthcare apps and app privacy assessment tools. This method of analysis of the literature for characteristics or gap analysis to identify aspects, which are missing in literature or other studies. Information from studies as 'result evaluations', quantitative data were combined with information from effective studies that represented mobile users' views influencing their privacy as 'views studies', qualitative data.

In this study, reviews are conducted in accordance with the phases of a mixed studies systematic review: setting the research questions or issues; searching studies or articles across a range of database sources; applying inclusion and exclusion criteria; assessing methodology; extracting data; and concluding with findings to answer the research questions. To accomplish this aim, comprehensive mapping and screening were used for identification of those studies which were most relevant for the research topic. The design was informed by the mixed method, which is shown in Figure 4. This represents the stages and processes of research review and research approach.

3.6. Data collection and analysis

The last stage of the Research Onion represents the techniques and procedures in which data collection and analysis is followed to answer the research issues. This study uses the qualitative data to answer the research questions. In this study, a total 760 studies were identified, in which only 23 studies of that total met the desired criteria of research and were included in the descriptive analysis.

Figure 4 has been removed due to copyright restrictions.

3.6.1. Search Method

In this research, all literature included in the study were searched from the Flinders University library 'Findit'. The search terms included health/medical subject and adapted accordance to the databases. The databases used for related studies were: IEEE Xplore, Science Direct, Emerald Fulltext, ProQuest, and Wiley Online Library. The main keywords selected for this search included "mobile health app privacy", "mHealth" and "issues in mobile health apps".

Apart from literature searches in ‘Findit’, references list of retrieved articles were searched to identify potentially relevant documents, which were then retrieved online.

3.6.2. Inclusion and exclusion criteria

Articles and other published works included in the study were based on the topics of information privacy and mobile health apps. Only studies that included both these search terms were used in the study. Studies were excluded if the studies were not matching the desired criteria for study or not directly relevant to mobile app privacy.

3.6.3. Screening

The identified studies were assessed by the review based on the title of the article or study and its abstract. Figure 5, which illustrates a Mixed Studies Review flow diagram, describes the flow of selecting studies at each step which is next discussed in detail in Chapter 4.

CHAPTER 4: RESULTS

This chapter represents literature reviews and discusses the information and data collection from various sources. The research process made under the keywords “mobile app privacy”, “mobile health app privacy”, “mHealth app privacy” and other articles that were containing these keywords. Articles were accessed from different databases by using the Flinders University portal.

4.1. Research Process

A mixed research process model represents a systematic order of steps of this study with the beginning of identification of the research problem and ending with identification of the results, discussion, and conclusion of the research.

Figure 5 has been removed due to copyright restrictions.

Figure 5 represents the research process for the representation of steps taken in the research of mobile app privacy assessment. First of all, the research started with introducing the research problem which was to determine how mobile apps handle privacy and can be assessed. Second, it defines the literature review related to this study, which identifies the privacy issues, principles of data protection and current ways to measure privacy in mobile apps. Third, it clarified the research problem and discussed the appropriate research method. In data collection, the author collected information relevant to the research problem from different sources from the university portal by using different database (i.e. IEEE, Science direct, Emerald Fulltext). After the collecting of data, data analysis was used to evaluate the useful data from selected studies from different sources. Then, the results were carried out on the basis of analysis.

4.2. Description of studies

In this study, a total 760 studies were identified for the purpose of finding the solution of research issues. This section represents the number of studies retrieved from 5 different databases. Figure 6 below summarises the research flow of the studies, which represents the inclusion and exclusion criteria of literature at different stages of this study.

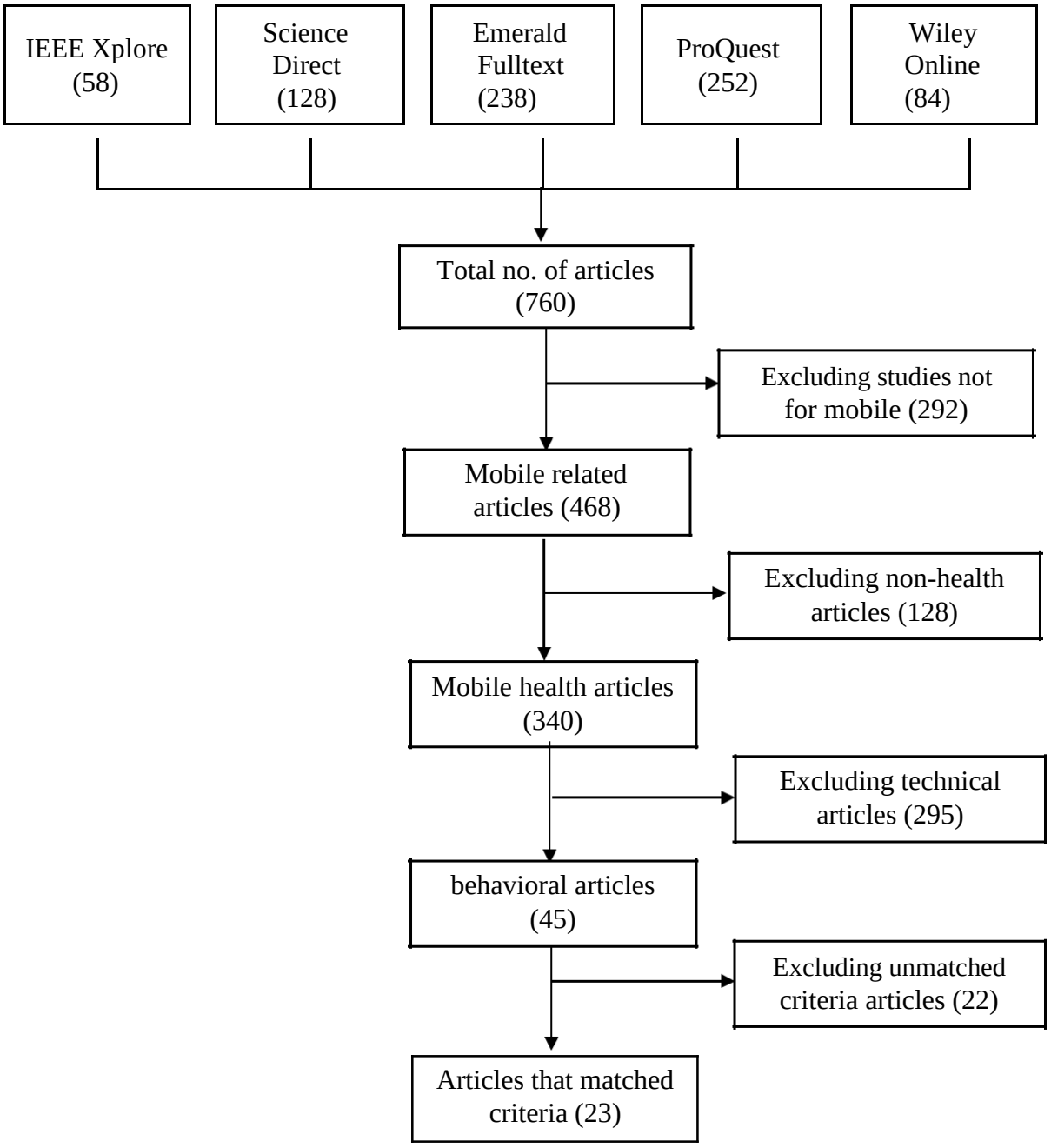

Figure 6. Flow diagram of research

Table 2 summarises the total number of studies reviewed from different databases between the published date range of from 2015 to 2019, for the purpose of finding the answer to the research questions. This range was selected because the most relevant and current information published over the past 5 years was required to give an up-to-date assessment of the present situation with health apps and privacy concerns of patients.

Table 2. Summary of reviewed studies from different databases

S. No.	Database	Terms	Total Number of Articles	Year	Type
1	IEEE Xplore	Mobile app health privacy	36	2015-2019	Conference Paper
			6	2015-2019	Journal Article
		Issues in mobile health apps	13	2015-2019	Conference Paper
			3	2015-2019	Journal Article
2	Science Direct	Mobile app health privacy	108	2018-2019	Research Article
			20	2018-2019	Review Article
3	Emerald Fulltext	Mobile app health privacy	181	2018-2019	Journal Article
			57	2018-2019	Book
4	ProQuest	Mobile app health privacy	241	2019	Journal Article
			11	2018-2019	Conference Paper
5	Wiley Online	Mobile app health privacy	64	2019	Journal Article
			20	2019	Book

4.3. Review of Selected Studies

Of the total of 760 articles, 737 studies were eliminated because those were not appropriately related or different to the area of purpose. Most studies were removed because studies were found to be inappropriately related to app privacy and not related to healthcare. For the purposes of the research, only relevant articles were considered as proper material for analysis. Therefore, a total of 23 articles of the mobile health app privacy were chosen as the material for further analysis because the inclusion criteria they covered were found relevant for the study. The main keyword for this selected studies was “mobile health app privacy”. This review can help the app developers to recognise the factors that may influence the intention of consumers from the concept of their data privacy on mHealth apps.

Table 3 describes the sorted research articles from different databases, which are reviewed for the assessment of mobile app privacy. These studies were used to answer the research questions. Results of the research study are based on the findings of these selected studies.

Table 3. Summary of articles reviewed and their details

S. No	Database	Terms	Name of Article	Authors	Year	Type	Summary
			Privacy Requirements for mobile e-Service in the Health Authority - Abu Dhabi (HAAD)	Asad M. Khattak ; Farkhund Iqbal ; Patrick C. K. Hung ; Jwo-Shiun Sun ; Guan-Pu Pan ; Jing-Jie Lin	2016	Conference Paper	This paper discusses data privacy requirements for Mobile e-Service at the HAAD in accordance with the HIPAA privacy requirements.
			Factors affecting disclosure of personal health information via mobile application	Kanokwan Atchariyachanvanich ; Nichaporn Mitinunwong ; Butsaraporn Tamthong	2017	Conference Paper	This paper explores the factors which affect personal health information disclosure though a mobile app in Thailand.
			Security and Privacy Analysis of Mobile Health Applications: The Alarming State of Practice	Achilleas Papageorgiou ; Michael Strigkos ; Eugenia Politou ; Efthimios Alepis ; Agusti Solanas ; Constantinos Patsakis	2018	Journal Article	This paper provides a security and privacy analysis of 20 popular mHealth apps, with tailored testing of each app functionality.
			A Taxonomy of mHealth Apps - Security and Privacy Concerns	Miloslava Plachkinova ; Steven Andrés ; Samir Chatterjee	2015	Conference Paper	This paper outlines issues related to mHealth apps. In this taxonomy was tested with 38 popular iOS and Android health apps.

1	IEEE Xplore	Mobile Health App Privacy	An OAuth2-based protocol with strong user privacy preservation for smart city mobile e-Health apps	Victor Sucasas ; Georgios Mantas ; Ayman Radwan ; Jonathan Rodriguez	2016	Conference Paper	This paper is based on OAuth2-based protocol that enables users authentication towards the e-Health services from the aspect of privacy.
			Trust4App: Automating Trustworthiness Assessment of Mobile Applications	Sheikh Mahbub Habib ; Nikolaos Alexopoulos ; Md Monirul Islam ; Jens Heider ; Stephen Marsh ; Max Müehlhäeuser	2018	Conference Paper	This paper introduces the Trust4App framework to consider the publicly available factors, such as ratings, user reviews, and number of downloads to distinguish benign from risky apps.
			Method for Selection of the Best Application for Women's Health	Jisan Lee ; Hyeongju Ryu ; Ahjung Byun ; Yeonji Ko ; Jeongeun Kim	2017	Conference Paper	This paper demonstrates a systematic analysis of the best app via assessment of the user's requirements.
			Privacy in Mobile Health Applications for Breast Cancer Patients	Jaime Benjumea ; Enrique Dorronzoro ; Jorge Ropero ; Octavio Rivera-Romero ; Alejandro Carrasco	2019	Conference Paper	This paper analyses the privacy policy in mHealth apps and develops a scale to test GDPR compliance.
			A systematic review of factors influencing the effective use of mHealth apps for self-care	Faiz Aiman Bin Azhar ; Jaspaljeet Singh Dhillon	2016	Conference Paper	This paper systematically reviews the factors that influence the usage of mHealth apps for self-protection.
			Authentication and Usability in mHealth Apps	Zhongwei Teng ; Peng Zhang ; Xiao Li ; William Nock ; Marcelino Rodriguez-Cancio ; Jules White ; Douglas C. Schmidt ; Denis Gilmore ; Jonathan C. Nesbitt	2018	Conference Paper	This paper discusses different authentication approaches that impact the usability of mobile health apps. Also, it presents metrics to evaluate common authentication approaches and impact on individuals.

			Are mHealth Apps Secure? A Case Study	Chiara Braghin ; Stelvio Cimato ; Alessio Della Libera	2018	Conference Paper	This paper analyses the issues of mobile health apps from the perspective of privacy and security requirements by different data protection laws and presents data protection by app.
			A Generic Process to Identify Vulnerabilities and Design Weaknesses in iOS Healthcare Apps	Christian DOrazio ; Kim-Kwang Raymond Choo	2015	Conference Paper	This paper proposed a generic process to identify vulnerabilities and design weaknesses in apps for iOS devices and proposed several recommendations to avoid the structural mistakes in future.
2	ProQuest	Mobile Health App Privacy	Secure Application for Health Monitoring	Bhuse, Vijay; Sinha, Harsh	2019	Conference Paper	This paper outlines the research aim of building secure and private Android app to monitor health using Bluetooth based sensors to track heart rate and blood pressure.
			Detection of Premeditated Security Vulnerabilities in Mobile Applications	Brilingaitė, Agnė; Bukauskas, Linas; Kutka, Eduardas.	2017	Conference Paper	This paper proposes a framework and methodology to detect security issues in mobile apps at various levels.
			An Overview of Cybersecurity Regulations and Standards for Medical Device Software	Lechner, Nadica Hrgarek	2017	Conference Paper	This paper presents current cybersecurity regulations and standards for medical device software set by government agencies and agencies developing industry and international standards and others.
			Smart Citizens Wanted! How to act Responsibly With Data Security and Privacy?	Ziske, Christine; Ziske, Ulf.	2019	Conference Paper	This paper proposed concept of the new protocols to improve the authentication.
			Reviewing the data security and privacy policies of mobile apps for depression	Kristen O'Loughlin, Martha Neary, Elizabeth C. Adkins, Stephen M. Schueller	2019	Research Article	This article presents the review of data privacy policies in apps for depression.

3	Science Direct	Mobile Health App Privacy	How private is your mental health app data? An empirical study of mental health app privacy policies and practices	Lisa Parker, Vanessa Halter, Tanya Karliychuk, Quinn Grundy	2019	Research Article	This article considers the insufficient attention of app industry to protect the privacy of mental health app users.
			Availability, readability, and content of privacy policies and terms of agreements of mental health apps	Julie M. Robillard, Tanya L. Feng, Arlo B. Sporn, Jen-Ai Lai, Roland Nadler	2019	Research Article	The key findings of this paper are data sharing and transparency related to mental health apps and importance of regulation in the mobile apps.
4	Emerald Fulltext	Mobile Health App Privacy	"Warning! You're entering a sick zone"	Scott S.D. Mitchell	2018	Research Article	This article describes the privacy implications of digital illness tracking tools.
			Health apps usage and preferences among Saudi patients with diabetes: A survey	Mohamed Rafiullah Satish Kumar David	2019	Journal Article	This article investigates Android health apps amongst diabetic patients in Saudi Arabia. Also, it discusses user preference and the challenges of using health app.
5	Wiley Online	Mobile Health App Privacy	Regulating mobile mental health apps	Nicolas P. Terry Tracy D. Gunter	2018	Article	This article defines the concerns with health apps and accessing app services without increasing risks.
			Privacy Issues in Smartphone Applications: An Analysis of Headache/Migraine Applications	Mia T. Minen Eric J. Stieglitz Rose Sciortino John Torous	2018	Article	This article examines the 29 most popular headache and migraine apps from the content of privacy policies.

Table 4 below represents the characteristics of reviewed articles including summary of purpose, methods, target area and reported results. Findings of these studies were helpful to find out results for our study. This represents how privacy in mobile apps is assessed by these studies, method selected for privacy assessment and level of data privacy assessment in apps.

Table 4. Characteristics of reviewed papers

Study	Name of study	Purpose	Target Area	Method	Results
(Agnė Brilingaitė, 2019)	Detection of Premeditated Security Vulnerabilities in Mobile Applications	Purpose is to analyse security of mobile apps at data handling, communication and source code levels. Track down premediated vulnerabilities design. The purpose of the experiment was to assess the security risk of the applications using our proposed methodology.	An experiment on a number of apps in four categories: networking, finance, messaging, and transportation apps. From each category, 10 most popular from different vendors were selected.	The schematic view of the methodology is presented. The methodology contains four phases: mobile device context (MDC), application context (AppC), software context analytics (SCA), and network context analytics (NCA).	Results indicate that messaging applications request the most significant number of total and dangerous permissions on average. The second largest number of dangerous permissions is in the category of finance apps, have the second largest number of total permissions on average. Such results are influenced by the specific use of hardware within the application. Results showed that even financial sector applications did not encrypt sensitive data on a device, tracked user behaviour, and did not follow the recommendations for good coding practices applicable in mobile application development.
(Hoppe, A. 2017)	Privacy Issues in Mobile Health Applications - Assessment of Current Android Health Apps	The presented study analyze privacy behavior of m health apps (i.e. pill reminder)	Analyzed 58 popular health apps from German Google play store.	Static analysis, permission analysis and dynamic analysis	Finding of study depicted that none of app samples fulfil the transparency of data accessibility and comprehensibility of privacy practices. Less than half number of apps directly links to their privacy policy statements in app. The purpose of user's data collection and processing are sometimes mentioned but are not elaborated. This shows that there is no clear idea where the user's data goes and who access their data.
(Azhar & Dhillon, 2016)	A systematic review of factors influencing the effective use of mHealth apps for self-care	This paper systematically reviews the factors that influence the usage of mobile health apps for self-care.	A total of 206 studies were selected for identification of factors that influences the usage of mobile healthcare application for self-care. 68 prominent factors based on influencing the effective usage of mHealth apps for self-	Literature review.	Findings can be helpful to mobile health app developers for he understanding of those factors that affecting the users to use the mobile apps effectively and developing effective mobile apps. It recommends some models (i.e. mobile adoption and the usage model, UTAUT2 and TAM2).

			care are discussed.		
(Benjumea, Dorronzoro, Ropero, Rivera-Romero, & Carrasco, 2019)	Privacy in Mobile Health Applications for Breast Cancer Patients	The purpose of study is to analyse the privacy policy of a selected mobile health apps for breast cancer and develop a scale to check if GDPR is compliance.	Study analyses total 9 mobile health apps related to breast cancer self-management, applying novel privacy assessment scale.	A systematic search was conducted. All relevant mobile health apps for breast cancer were identified on Google Play and Apple Store.	Around 60% apps did not show any issue with their privacy policies. 40% apps have 50% or higher privacy policies score. The highest privacy policies score reaches around 80% and the lowest one only score is 25%.
(Bin Li, A System for Privacy Information Analysis and Safety Assessment of iOS Applications, 2015)	A System for Privacy Information Analysis and Safety Assessment of iOS Applications	This study analysed the security status of apps and proposed a scheme-analyse the security assessment system to detect the information leakage.	Analysis of iOS apps	App security analysis including statics, dynamic and Security Level Scoring Algorithm (SLSA).	Automatic detection system to detect application of Apps to define the privacy issues in app to ensuring the privacy of user data. In (SLSA), correspondence value for privacy API will be defined. When a app leaks privacy data, the correspondence values will be recorded. Lastly, all values are added to get a total score, so that the security level accordance to the total score can be judged.
(Chiara Braghin, 2018)	Are mHealth Apps Secure? A Case Study	Analyze the security issues of mHealth apps from the perspectives of GDPR or HIPAA, and the protocols and cryptographic techniques to guarantee the data security.	Analyze android and iOS apps related to health & fitness to reveal transparency, confidentiality and integrity and data security. For testing LG-G3 (running Android 5.0) is used.	Case study - a fitness tracker, steps; Analysis of the app privacy policy; Static analysis Analyse the BLE traffic between the smartphone and fitness tracker.	Finding demonstrates that there are many applications that do not meet the expected standards for privacy and security, therefore these are endangering their users' personal information.
(DOrazio & Choo, A Generic Process to Identify Vulnerabilities and Design Weaknesses in iOS	A Generic Process to Identify Vulnerabilities and Design Weaknesses in iOS Healthcare Apps	This study proposes a process to identify the design issues in iOS apps.	Study validates process with a widely used Australian Government Healthcare app and reveals previously unknown or unpublished vulnerabilities of mobile devices.	Study proposed analysis process of iOS apps, including Static analysis and Dynamic analysis	Findings highlighted that iOS the implementation of security mechanisms (i.e. anti-debugging techniques) that could increase the user’s data protection of in mobile systems.

Healthcare Apps, 2015)					
(Habib, et al., 2018)	Trust4App: Automating Trustworthiness Assessment of Mobile Applications	In this study, Trust4App framework for assessing trustworthiness for mobile apps is introduced.	Study assess top 20 free apps from 7 different categories. To validate its framework, study tests it on apps available on the Google Play store.	Study assess the app's reliable trustworthiness. In this, static analysis, statistical techniques, and computational trust methods that produce trustworthiness scores.	Trust4App framework considers the permission factor as privacy to assessing the quality of software and reduce privacy and security threats.
(Julie M. Robillard, 2019)	Availability, readability, and content of privacy policies and terms of agreements of mental health apps	To assess the app availability, terms of agreement and privacy policies of mental health apps.	Most famous 100 smartphone apps related to 'track' and 'mood' apps were evaluated.	Availability of terms of agreement and privacy policy in iOS and Android apps is accessed	Most apps were not including terms of agreement and privacy policy. Almost 20% of iOS apps and around 5% of Android apps following privacy policies, whereas 15% and 3% of iOS and Android apps following terms of agreement. Many privacy policies of 71% iOS and 46% Android apps stated that users' data may be shared with third parties .
(Kristen O'Loughlin, 2019)	Reviewing the data security and privacy policies of mobile apps for depression	Study reviews data security and privacy policies in mobile apps related to depression.	Study identified 116 iOS and Android apps	Apps were retrieved and evaluated the handling procedures and transparency of data	According to research, 79% of apps were collecting identifiable data have a privacy policy whereas 34% apps were collecting only non-identifiable user's data.
(Lechner, 2017)	An Overview of Cybersecurity Regulations and Standards for Medical Device Software	This paper discusses Present cybersecurity regulations and medical device software set by government agencies and agencies developing industry and international standards such as the FDA, CFDA, ISO, IEC, UL, etc.	The concepts described within this paper can be utilized by medical device manufacturers in order to establish a program as part of their quality management systems.	There are three complementary ways based on the NIST (National Institute of standards and Technology) cybersecurity framework that can be used to remove gaps in the organization 's cybersecurity. The first way focuses on designing software products that take cybersecurity into	Finding of paper recommend Software testers and IT infrastructure personals to integrate security testing in their testing procedures and to gain knowledge about security testing tools and latest cyber vulnerabilities of hardware and software.

				account (i.e., prevention). The second way is to perform security and penetration testing and to apply other cybersecurity controls to reduce attacks and vulnerabilities that could be exploited (i.e., detection). The third way emphasizes maintenance plan in case of a cyberattack (i.e., response and recovery).	
(Mia T. Minen, 2018)	Privacy Issues in Smartphone Applications: An Analysis of Headache/Migraine Applications	To examines the most popular headache and migraine apps from the content of privacy policies, to assess privacy issues.	Total 29 apps (14 diary related apps, 15 relaxation related apps) were selected	In this, systematic search of apps is conducted to examine the privacy policies in apps.	Around 80% (11 out of 14 diary apps) apps had privacy policies. Total 55% (6 out of 11 apps) state that some user data was used to serve targeted advertisements. Almost 70% (11 out of 15 relaxation apps) apps had privacy policies.
(Mitchell, 2019)	"Warning! You're entering a sick zone"	This paper examine the privacy implications of digital illness tracking tools.	In this, analysis of Sickweaher and HealthMapp apps is used.	Study performs a content and platform analysis. This analysis use a cultural-historical activity theory framework and walkthrough method.	Author argues that disease tracking apps compelling users to submit their personal information, including sensitive health information with less regulation.
(Mohamed Rafiullah, 2019)	Health apps usage and preferences among Saudi patients with diabetes: A survey	The purpose of study is to assess the usage pertaining patterns to different Android health apps related to diabetic patients in Saudi Arabia and patient preferences to use health apps and challenges.	Investigates the patterns of smartphone use, examines the usage of mobiles for health and assess the patient preferences for health related use of mobile phone apps.	A cross survey based on close-ended structured questionnaire and a self-administered methods are conducted.	More than a third of the respondents who were surveyed found easy to understand health apps and an equal number of respondents needed some training to use apps. Around 30% of the participants did not want to know about their health. However, almost 50% participants were unsure of how to use health apps.

(Nicolas P. Terry, 2018)	Regulating mobile mental health apps	This article focusing on the data protection, safety and quality issues of mHealth apps and exploring the approaches taken by regulatory agencies.	Study the patient-facing mobile medical apps and provider-facing technologies	Literature review	Risk-assessment of literature recommend that regulatory agencies are less helpful to develop working risk frameworks for the assessment of mobile medical apps.
(Lee, Ryu, Byun, Ko, & Kim, 2017)	Method for Selection of the Best Application for Women's Health	Study provides a systematic analysis method of apps by assessing the user's requirements.	Study examines the top 5 apps that available on iOS and Android platform. These apps are evaluated by app developers and experts. Study conduct group interviews with women in their 20s and 30s who experience dysmenorrhea.	In this study a systematic analysis method is selected	Random trials of using this methodology by medical experts can help for the care of women who are suffering from dysmenorrhea. Its results can play an important role in demonstrating the mechanism by which mobile health can benefit to disease.
(Li Li, 2016)	Static Analysis of Android Apps: A Systematic Literature Review	Objective of this study is to provide a view of static analysis to assess the security of mobile apps and report limitation of analysis	Total 92 publications related to Android, based on statics analysis were selected. This review is performed to address static analysis sensitivities and considered android characteristic.	A systematic literature review	Most studies support various analysis sensitivities but there are very less consider to path sensitivity No any single work is proposed to track all challenges of static analysis of Android Very a small section of related works have made their artefacts publicly available.
(Lisa Parker, 2019)	How private is your mental health app data? An empirical study of mental health app privacy policies and practices	This study identifies the threats related to mental health apps privacy and recommendations to promote consumer interest.	Total 61 of mental health apps are selected.	Study analyze a critical content analysis	Most of apps encourage users to share their data over internet. It examines that around 50% applications do not discuss a privacy policy.
(Papageorgiou, et al., 2018)	Security and Privacy Analysis of Mobile Health Applications: The Alarming State of Practice	To evaluate how apps are handle, request and disseminate the sensitive personal information.	Total 20 health apps were selected	App collection Static code analysis and dynamic analysis of app	Majority of the assessed apps has been found that apps do not follow well-known data protection guidelines and legal regulations. Most popular mHealth apps can leak users' sensitive data such as health data, emails, etc.

(Plachkinova, Andrés, & Chatterjee, 2015)	A Taxonomy of mHealth Apps - Security and Privacy Concerns	Study outline the issues related to creating and downloading of mobile health apps.	Total 38 most popular Android and iOS m-health apps are assessed.	Literature review	This study followed the quantitative content analysis methods to improve the quality of the study. In this combine this research method with Hevner's recommendations
(Stoyan, et al. 2015)	Mobile App Rating Scale: A New Tool for Assessing the Quality of Health Mobile Apps	Aim of the study is to measure and classify the quality rating of mHealth apps.	Total 60 popular apps were assessed using iTunes and 25 publications were selected.	A literature search was used to identify the studies to assess quality rating criteria from January 2000- 2013. Mobile App Rating Scale (MARS)	MARS provided a checklist for designing and developing high quality m-health applications.
(Teng, et al., 2018)	Authentication and Usability in mHealth Apps	Study purpose different authentication approaches to evaluate how these impact the mobile health apps usability, and analyse how to vary authentication and CPI establishment architectures.	Study presents the metrics to evaluates the authentication approaches for mobile health apps.	This paper complements existing authentication literature by defining metrics for analyzing authentication approaches. This study proposed authentication method for mHealth apps, which helps overcome implications faced by health apps users.	Results of study reveal that username or password authentication approaches. Also, there is need improvements of SMS and OPT authentication.
(Tobias Dehling, 2015)	Exploring the Far Side of Mobile Health: Information Security and Privacy of Mobile Health Apps on iOS and Android	This study establishes an overview of iOS and Android mobile health apps to focus on potential issues by information privacy infringements.	Total 24,405 mobile health apps ware identified. 17,979 apps are used for assessment of privacy infringements.	Study assess the health & fitness app offered on iOS and android platform.	Findings show that 95% apps have at least some potential damage by information privacy infringements. There are 2098 apps out of 17,979 which has high potential damages.

4.4. Mobile health app privacy assessment

Table 5 below summarizes the whole chapter and discuss the solution of research questions 1 and 2 which were raised in section 1.3.

4.4.1. Research question 1

Research question 1 is divided into two parts- part 1 and part 2. Part 1, how do mobile apps for health handle privacy? Part 2 is, can the level of privacy be assessed? Firstly, we will discuss present the solution for part 1, then part 2.

Part 1: Methods to assess privacy handles by mHealth apps

Some of selected studies focused on assessment of mobile apps. Hoppe et al. (2017) analysed the static and dynamic analysis to assess current Android health apps. In static analysis, authors analysed the data flow in mobile app components. Their study discussed ApkCombiner tool to detect data privacy leakage in apps. Authors have reviewed the legal documents that are accompany the software products that treat user's personal data. Their study helped to provide useful information to find solution of research questions of this study. This part discusses the methods to know about how privacy is handled by mHealth apps. This represents static, dynamic and permission analysis methods to assess privacy in apps which can help app users to gain information about how the mHealth apps are handling privacy of their data.

- **Privacy by design**

Privacy by design (PBD) approach aims to build privacy and protecting data in the design specification and architecture of information systems and technologies to provide data protection. An app developer develops PBD approach in mobile apps by using privacy enhancement practices in the lifecycle of personal data which is handled as data collection, data usage, data disclosure and storage. PBD helps to provide privacy in apps even when app is not covered by Privacy Act.

- **Privacy Policy:**

Hoppe et al. (2017) discussed that privacy policies and guidelines find out a mobile app comply with the legal standards to use user data. Privacy policy is legal requirement for all applications and organization to protect their consumer’s personal data. Privacy policy in mHealth apps address the user data management, data processing, data privacy and security, data breach notifications and data access rights to app users. Mia et al., (2018) also presents privacy policies to assess privacy in mHealth apps.

Australian Privacy Principles (APP): APP defines how personal data should be handled by an app. This provides flexibility to an organization or app to handle personal data of their users (OAIC, 2014). APP principles cover usage, collection, storage and disclosure of personal data in apps. This allows app users to access, control and modify their data in an app. There are total 13 APPs which are mentioned in this work in the section 2.8.2. There are some specific APPs that deal with data handling. App 3 is applied to the collection of sensitive data, APP 6 discloses and usage of personal data. APP 7 discloses personal data usage and disclosure for direct marketing, whereas APP 8 deals with cross border disclosure of personal data (OAIC,2014).

General Data Protection Regulation (GDPR): In Australia, organisations and apps which comply with European Union's GDPR, privacy policy also needs to comply with requirements of GDPR. This allows app users to control their personal data in an app or organizational environment. GDPR in apps can be assessed by various tools, such as Opus Global's third party compliance tool. This tool provides solution to identify the third parties with whom user's personal information is shared and how it is shared (Jackson, 2017). Hoppe, et al. (2017) analysed the GDPR Act in their study that discuss about protecting user data from privacy and data breaches. Their study discusses that user's personal information is strictly prohibited to process and collect without the permission by law. Under the GDPR act, apps should provide necessary information about transparency of use, collect and process user data should be provided and mechanisms should be provided, so user could modify, review or delete their collected data (Hoppe, et al. 2017).

FDA guidelines: FDA encourages the mobile health apps developers to search product classification and pre-market notification database to define the level of regulation in an app. FDA applies risk based approach to mobile apps to ensure safety and effective use of devices. FDA regulates moderate risk and high risk devices functions (Lechner, 2017).

Part 2: Levels of mobile health app privacy

Levels of privacy assessment in mobile health apps are mentioned in Figure 7. Mobile app privacy is divided into three levels.

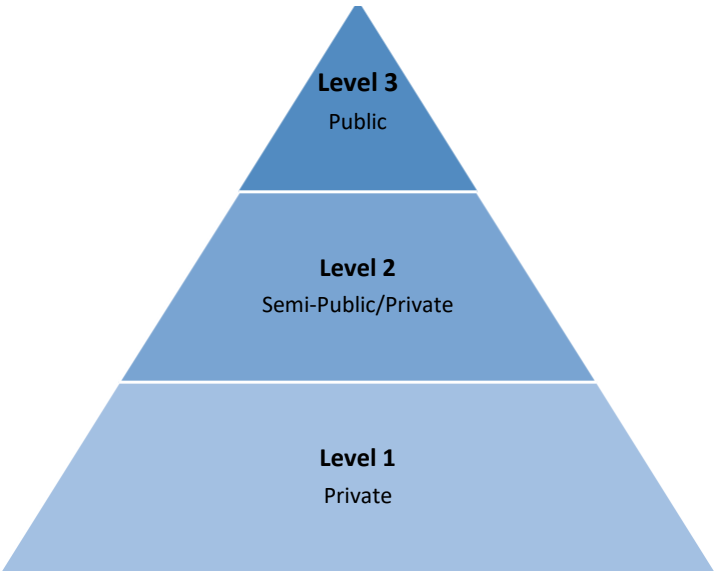

Figure 7. Pyramid of privacy levels in apps

Pyramid of privacy levels is used to represent low, medium and high level of privacy. Level 1 defines high level of privacy, whereas level 2 and level 3 defines medium and low level privacy, respectively.

Level 1 represents the high level of app privacy. This level of privacy presents Private data, such as authentication and authorization of user data in mobile apps. Authorization allows authorized user to modify their data such as read or write data. Authentication demonstrates the privacy of user login in an app including username and password. User password for app login is most sensitive information. Using strong passwords (password that includes uppercase and lowercase alphabets, numbers and special keywords) are good option to protect health data in mobile apps. Sometimes, it is harder to remember passwords, however the password management can be used to memorize such passwords. Kaspersky password manager can be used to protect passwords in Apple iPhone and Android devices. This password manager keeps user login and password details in a secure vault and use them in corresponding fields of websites. Level 2 defines the semi-public or private data which user wants to share their data with some special group of users, such as friends. This level has medium level of privacy. Level 3 demonstrates the public access of user data in app, such as user's photo. This data has low level privacy and easily accessed by unauthorized person as hacker.

Figure 8 below represents the example of user data privacy levels in Fitbit mobile app, which represents who is allowed to access user's data in app either only user, friends or anyone.

Figure 8 has been removed due to copyright restrictions.

4.4.2. Research question 2

The second research question is "What would a mobile app privacy assessment tool for consumers look like?" To answer this question, first we will discuss some privacy tools, and then presents the answer of second research question.

- **Mobile app privacy tools:** Tools that used in mobile apps for protecting user data are Password manager, Virtual private network and Two factor authentication (Kounelis et al. 2012). These are briefly mentioned as below;
  1. Password Manager: Password manager tools are used to protect user login details, specially passwords such as, 1Password and Dashlane. These password managers are as secure password storage vault that secure the user details such as personal data, payment methods and receipts in apps.
  2. Virtual Private Network (VPN): Virtual Private Network is a privacy guardian that allows user to connect to internet via a private encrypted tunnel which minimize the changes of data threat. VPN allows the data communication over an internet by encrypting data to secure it from hackers or internet services providers or other parties. In Australia, ExpressVPN is one of best VPN service providers which is most secure and reliable. ExpressVPN provides the feature of DNS (Domain Name Server) leakage protection.
  3. Two-Factor Authentication (2FA): Two factor authentication in mobile apps is a security measure which protect device data. This authentication ensures to user that he is the only person that can access his data by verifying account. In a case, if a mobile device is stolen then it prevents another user from accessing user account details.

- **App privacy assessment tools:**
  App privacy assessment tools help users to assess privacy in mobile health apps. These tools can be used to assess privacy of mobile apps.

1. Quality Management: Quality management is most prominent tool to assess privacy in apps. Quality of an app can be managed by Privacy policy and Terms and Conditions to use user data (Hoppe et al., 2017). This represents how user data will be used and with whom it might be shared through the app. Privacy policy and terms of conditions of an app can help app user

to understand how app stores and use their data. Stoyan, et al. (2015) has proposed MARS as a tool to assess the quality of mHealth apps. MARS is a reliable tool to assess quality and develop high quality of apps (Stoyan, 2015).

2. User Services: User services in mobile apps allow user to control over their data. Figure 8 above represented an example of a Fitbit app. Its privacy feature allows its users to what and who could access their personal data.

3. App Rating and Reviews:

   App rating and reviews tools can help users to know about reliability of an app (Stoyan, et al. 2015). App rating and reviews are represented by number of stars. Higher star (4/5 or 5/5 stars) rating represents good user engagement in app, and lower star rating (less than 3 stars) describes worst user interaction with app.

4. Laws Confirmation: Law confirmation in apps by APP (Hoppe, et al. 2017) and FDA (Maged N. Kamel Boulos, 2014) presents how data is processed in apps and with whom it can shared or accessed.

CHAPTER 5: DISCUSSION

After the extraction of resources from different databases, author have shortlisted the how privacy in health mobile apps is handled and tools to assess privacy. The answers of the research questions are made on the basis of the information gathered from resources.

5.1. Principle findings

This paper evaluated the reviewed studies to find solution of research issues. These findings are important because these suggest assessment of data privacy in mobile apps. It may guide users to conduct privacy assessment for protecting personal information in apps. However, this study is based on reviewed studies of which, a very less number of studies focused on privacy assessment, and thus, an area of app privacy assessment should be explored in future.

Main finding to this work is to address research questions. This study examined two research questions:

Research Question 1: How mobile health apps handle privacy and can level of privacy be assessed?

Most of reviewed studies presents systematic review to assess mHealth apps. Mia et al., (2018) conducted systematic search to examine the privacy policies in mHealth apps by systematically assessing 28 apps top rated apps of headache and migraine. Hoppe et al. (2017) analysed the static and dynamic analysis to assess mobile health apps in their study. Their study provided useful information to find solution of research questions for our study. Privacy policy and legal guidelines of apps provides information to users about how their data is processes and collected by an app (Hoppe et al.,2017). Another study by Benjumea (2019) analyzed the privacy of data in mHealth apps by using systematic review (Benjumea, Dorronzoro, Ropero, Rivera-Romero, & Carrasco, 2019). This study assess privacy by conducting a scale to check GDPR compliance.

Research Question 2: What are the app privacy assessment tools look alike to consumers?

To answer the research question 2, study by Stoyan, et al. (2015) has proposed MARS as a tool to assess the quality of mobile health apps, which is a reliable tool to assess quality and develop a new high quality app (Stoyan, 2015). Kounelis, et al. (2012) proposed a mobileak project in their study for the assessment of mobile apps. Not much information is provided by reviewed studies for app assessment tools. Adjunct study of assessment tools is still required. On the basis of studies, app privacy assessment tools such as quality management, identifications of issues, tools and technology, user services, app reviews and rating and laws confirmation are briefly presented in the Results chapter 4.

5.2. Limitation of study

As determined by the use of a mixed study method, a literature review presents the studies of privacy assessment in healthcare apps. Limitation of method is that mixed study method is a time consuming method. This study is quite specific and did not conduct any real research experience. Therefore, the study perspectives are limited and highly dependent on research conducted in reviewed articles by their authors whose views and findings are their own. However, despite this limitation, the research results can be helpful in comparing and corroborating information from studies in the literature to gain a comprehensive view.

CHAPTER 6: CONCLUSION

Mixed studies review methodology makes a prominent contribution to health research. From the discussion, it can be concluded that there are currently a number of important privacy issues with the use of mobile applications in health. The use of mobile applications in healthcare services has become popular and has improved the management of service delivery for patients as well as benefiting the work of healthcare professionals. This is particularly true for some individuals and communities, such as those living in remote areas with limited access to hospitals and medical professionals. However, the inadequacy of provisions for security and privacy in mobile applications has compromised the trustworthiness of services in the healthcare system and exposed users to privacy intrusions and collection of their personal information without their knowledge. Privacy policies of apps are weak, have poor rates of availability, correlation of app ratings, and leakage of private details of users. The findings of this study draw together, provide correlations, and enhance the results of the previous body of research on mobile health app privacy assessment that consistently points out the dangers of health apps. The findings of this research can therefore be useful for health app users and app developers by encouraging improved methods of protecting user data privacy. It will be helpful to app developers and privacy regulating authorities to better understand the concept of privacy in health apps and will be helpful for app users and developers to make better data privacy decisions.

Mobile apps represent higher risks because users are likely to naively download and install apps without being aware of the risk of having their personal data shared with others or of being vulnerable to hacking by cybercriminals. There are some particularly serious privacy risks and cybersecurity threats presented by apps, which can impact users through theft of personal information or intrusions of malware or other viruses. Apart from the app sharing personal data on users without their knowledge or approval, apps can expose users to malicious attacks that can jeopardise their health and wellbeing. Apps have inherent security deficiencies that can be exploited by online thieves, including the collecting of passwords; collecting credit card or debit card numbers; collecting personal information, such as disease status, disease symptoms, and medical diagnoses; retrieving email contents, and remotely activating cameras on devices (Tuohy et al, 2013).

To assess the mobile application privacy risk, privacy professionals or another mobile app can be employed. This other mobile can be termed as a privacy professional, which can analyse the information on the main mobile app third party domains, data can be collected, cookies received, data stored on other devices, which can result in insecure data transmission or unauthorised permissions. By analysing these information contents, the mobile app can be rated as high risk, low risk, or medium risk, and that advice can be useful for any person considering

downloading an app. Privacy professionals assess the risk and rate the app as per privacy laws and regulation compliance standards.

Limitations and Future work

In this research a total of 23 recent studies were included. However, only a proportion of these articles, less than half, included much assessment of privacy in health apps and provided information of research issues on assessment. Therefore, there were difficulties in making the results more comprehensive due to a shortage of specific studies on assessment of health app privacy. As this is a very new area of research with more interest and research coming forth each year, it is hoped that future research can focus on the subject of assessment of app privacy to enable better solutions to this problem.

REFERENCES

Achilleas Papageorgiou, M. S. (2018). Security and Privacy Analysis of Mobile Health Applications: The Alarming State of Practice. *IEEE, 6*(2169-3536), 9390-9403.

Agnė Brilingaitė, L. B. (2019). Detection of Premeditated Security Vulnerabilities in Mobile Applications. ProQuest.

Armerding, T. (2018, December 20). *The 18 biggest data breaches of the 21st century*. Retrieved 2019, from CSO: https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the- 21st-century.html.

Armerding, T. (2018, December 20). *The 18 biggest data breaches of the 21st century*. Retrieved 2019, from CSO: https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html.

Alvesson, M., & Skoldberg, K. (2017) *Reflexive methodology: New vistas for qualitative research*. USA: Sage.

Azhar, F. A., & Dhillon, J. S. (2016). A systematic review of factors influencing the effective use of mHealth apps for self-care. IEEE.

Benjumea, J., Dorronzoro, E., Ropero, J., Rivera-Romero, O., & Carrasco, A. (2019). Privacy in Mobile Health Applications for Breast Cancer Patients. IEEE.

Bin Li, Z. F. (2015, November 19). A System for Privacy Information Analysis and Safety Assessment of iOS Applications. *International Conference on Security and Privacy in Communication Networks*, pp. 392-398.

Braun, V., Clarke, V., Hayfield, N., and Terry, G. (2019) Thematic analysis, *Handbook of Research Methods in Health Social Sciences*, pp. 843-860.

Chiara Braghin, S. C. (2018). Are mHealth Apps Secure? A Case Study. IEEE.

Cawley, C. (2018, March 1). *5 Apps Doing a Terrible Job of Protecting Your Privacy*. Retrieved April 2019, from Tech.co: https://tech.co/news/5-apps-trrible-job-protecting-privacy-2018-03

Dongjing He, M. N. (2014, Nov 14). Security Concerns in Android mHealth Apps. *NCBI*, 645-654. Retrieved from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4419898/

DOrazio, C., & Choo, K.-K. R. (2015). A Generic Process to Identify Vulnerabilities and Design Weaknesses in iOS Healthcare Apps. ProQuest.

Dredge, S. (2013, September 03). *Yes, those free health apps are sharing your data with other companies*. Retrieved April 2019, from The Guardian: https://www.theguardian.com/technology/appsblog/2013/sep/03/fitness-health-apps-sharing-data-insurance.

Editors, e. (2017, December 06). *eMarketer Updates Worldwide Internet and Mobile User Figures*. Retrieved March 2019, from eMarketer https://www.emarketer.com/content/emarketer-updates-worldwide-internet-and-mobile-user-figures.

FPF, C. (2011, 01). *Best Practices for Mobile Application Developers.* Retrieved 2019, from FPF: http://www.applicationprivacy.org/wp-content/uploads/2011/01/Mobile-App-Packet_Final.pdf.

Grant MJ, Booth A. A typology of reviews: an analysis of 14 review types and associated methodologies. Health Info Libr J. 2009 Jun; 26(2):91–108.

Hamed, A., & Ayed, H. K. B. (2016, November). Privacy risk assessment and users' awareness for mobile apps permissions. In *2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA)* (pp. 1-8).

Habib, S. M., Alexopoulos, N., Islam, M. M., Heider, J., Marsh, S., & Müehl, M. (2018). Trust4App: Automating Trustworthiness Assessment of Mobile Applications. IEEE.

Heydari, M., Sadough, S. M. S., Farash, M. S., Chaudhry, S. A., & Mahmood, K. (2016). An efficient password-based authenticated key exchange protocol with provable security for mobile client–client networks. *Wireless Personal Communications*, *88*(2), 337-356.

Hoppe, A., Knackmuß, J., Morgenstern, M., & Creutzburg, R. (2017). Privacy Issues in Mobile Health Applications-Assessment of Current Android Health Apps. *Electronic Imaging*, *2017*(6), 76-83.

Intelligence, M. (2019). *Mobile health (mhealth) market - growth, trends, and Forecast (2019 - 2024).* Retrieved from https://www.mordorintelligence.com/industry-reports/mobile-health-market.

Jacinto, A. F., Brucki, S., Porto, C. S., Martins, M. D. A., and Nitrini, R. (2011) Detection of cognitive impairment in the elderly by general internists in Brazil, *Clinics*, 66(8), pp. 1379-1384.

Jackson, W. (2017). 11 top tools to assess, implement, and maintain GDPR compliance. *CSO.*

Jonathan Shepherd, R. R. (2005, November). *Young People and Healthy Eating: A Systematic Review of Research on Barriers and Facilitators*. Retrieved from ResearchGate.

Julie M. Robillard, T. L.-A. (2019). Availability, readability, and content of privacy policies and terms of agreements of mental health apps. *Elsevier, 17*(100243).

Kearns, J. (2017). *Data-protection-principles-gdpr-serveit.com*. Retrieved April 2019, from Tucr io: https://tucr.io/gdpr-advice-for-retail-and-hospitality-businesses/data-protection-principles-gdpr-serveit-com/#.XLMuNTAzbIU.

Kounelis, P. S. a. I., 2012. *The mobileak project: Forensics methodology for mobile application privacy assessment.* London, IEEE Xplore, pp. 297-303.

Kristen O'Loughlin, M. N. (2019). Reviewing the data security and privacy policies of mobile apps for depression. *ScienceDirect, 110-115*, 15.

Kumar, R. (2019) *Research methodology: A step-by-step guide for beginners*. USA: Sage.

Lawrence, B. (2017, April 13). *Health care and mobile man-in-the-middle risks: Guidance for HIPAA-covered entities*.

Lechner, N. H. (2017). An Overview of Cybersecurity Regulations and Standards for Medical Device Software. ProQuest.

Lee, J., Ryu, H., Byun, A., Ko, Y., & Kim, J. (2017). Method for Selection of the Best Application for Women's Health. IEEE.

Li Li, T. F. (2016). *Static Analysis of Android Apps: A Systematic Literature Review.* Germany.

Lisa Parker, V. H. (2019). How private is your mental health app data? An empirical study of mental health app privacy policies and practices. *Elsevier, 64*, 198-204.

Mackey, A., and Gass, S. M. (2015) *Second language research: Methodology and design*. USA: Routledge.

McCusker, K., and Gunaydin, S. (2015) Research using qualitative, quantitative or mixed methods and choice based on the research, *Perfusion*, 30(7), pp. 537-542.

McGrath, P. (2019, August 8). *HealthEngine, medical booking app, facing multi-million-dollar fines for selling patient data*. Retrieved from ABC NEWS: https://www.abc.net.au/news/2019- 08-08/healthengine-facing-massive-fine-after-abc-investigation/11394564

Medium. (2019). *App Store vs Google Play: Stores in Numbers*.

Mia T. Minen, E. J. (2018). Privacy Issues in Smartphone Applications: An Analysis of Headache/Migraine Applications. *Headache*, 1014–1027.

Mitchell, S. S. (2019). "Warning! You're entering a sick zone". *Emerald Insight*, 1046-1062.

Mohamed Rafiullah, S. K. (2019). Health apps usage and preferences among Saudi patients with diabetes: A survey. *Int J Clin Pract*.

Mugge, K. T. &. C., 2014. *Security, Privacy & HIPAA for mHealth.* [Online] Available at: https://www.slideshare.net/javapro13/security-privacy-compliance-for-mhealth-apps-2014-isrm- conference 2014? qid=f7312e1e-18b0-4aa1-a4f1-e37eb785422d&v=&b=&from_search=14.

Mylonas, A., Gritzalis, D., Tsoumas, B., & Apostolopoulos, T. (2013, August). A qualitative metrics vector for the awareness of smartphone security users. In *International Conference on Trust, Privacy and Security in Digital Business* (pp. 173-184).

Nicolas P. Terry, T. D. (2018). *Regulating mobile mental health apps.* John Wiley & Sons.

Oliver, S., Harden, A., Rees, R., Shepherd, J., Brunton, G., Garcia, J. & Oakley, A. An emerging framework for integrating different types of evidence in systematic reviews for public policy. Evaluation & the Health Professions 2005, 11, 428– 66.

Palinkas, L. A., Horwitz, S. M., Green, C. A., Wisdom, J. P., Duan, N., & Hoagwood, K. (2015). Purposeful Sampling for Qualitative Data Collection and Analysis in Mixed Method Implementation Research. *Administration and policy in mental health*, *42*(5), 533–544.

Papageorgiou, A., Strigkos, M., Politou, E., Alepis, E., Solanas, A., & Constantino. (2018). *Security and Privacy Analysis of Mobile Health Applications: The Alarming State of Practice.* IEEE explore.

Pittman, D. (2014). 5 Problems with Mobile Health App Security. *MedPage Today*.

Plachkinova, M., Andrés, S., & Chatterjee, S. (2015). *A Taxonomy of mHealth Apps -Security and Privacy Concerns.* IEEE.

Ragan, S. (2015, February 4). Anthem confirms data breach, but full extent remains unknown. *CSO*. Retrieved 2019, from https://www.csoonline.com/article/2880352/anthem-confirms-data-breach-but-full-extent-remains-unknown.html.

Robson, C. (2011) *Real world research.* (3rd ed.) USA: Wiley.

Rosenfeld, L., Torous, J., & Vahia, I. V. (2017). Data security and privacy in apps for dementia: an analysis of existing privacy policies. *The American Journal of Geriatric Psychiatry*, *25*(8), 873- 877.

Rozepz. (2018, May 28). *Google Apps Privacy Issues? Everything You Need to Know*. Retrieved April 2019, from tom's guide: https://forums.tomsguide.com/faq/google-apps-privacy-issues- everything-you-need-to-know.191981

Sampat, B. H., & Prabhakar, B. (2017). Privacy Risks and Security Threats in mHealth apps. *Journal of International Technology and Information Management*, *26*(4), 126-153

Sealpath. (2014, August 25). *Protecting the three states of data*. Retrieved May 2019, from Sealpath: https://www.sealpath.com/protecting-the-three-states-of-data/

Silverman, D. (2016) *Qualitative research*. USA: Sage.

Stoyan R Stoyanov, L. H. (2015). *Mobile App Rating Scale: A New Tool for Assessing the Quality of Health Mobile Apps.* Australia: PMC.

Teng, Z., Zhang, P., Li, X., Nock, W., Rodriguez-Cancio, M., White, J., & C., D. (2018). Authentication and Usability in mHealth Apps. IEEE.

Tobias Dehling, F. G. (2015). *Exploring the Far Side of Mobile Health: Information Security and Privacy of Mobile Health Apps on iOS and Android.* Germany: JMIR Publications.

Vijay Bhuse, H. S. (2019). Secure Application for Health Monitoring. ProQuest.

Wakefield, J. (2014). *eBay faces investigations over massive data breach.* BBC News. Retrieved 2019.

Waller,L. R. (2011, August 19). *The Research Process.* Retrieved from https://guides.lib.usf.edu/c.php?g=291297&p=2104188##targetText=The%20research%20process%20involves%20identifying, or%20put%20together%20a%20presentation.

Zhao, S., et al. (2018). *Exploiting Proximity-Based Mobile Apps for Large-Scale Location Privacy Probing.* Security and Communication Networks.

Ziske, C. Z. (2019). Smart Citizens Wanted! How to act Responsibly with Data Security and Privacy? ProQuest.