

Privacy and Security Risks of the Top mHealth Applications for Headache Disorders

By

Ashley Burgess

Information Security & Intelligence, B.S.

Ferris State University, 2015

Advisor:

Dr. Greg Gogolin, Ph.D.

Full Professor

Accounting, Finance, and Information Systems Department

Spring, 2018

Ferris State University

Big Rapids, MI

Copyright: 2018 Ashley Burgess

All Rights Reserved

DEDICATION

I would like to dedicate this project to my family, who has endured some of life's toughest challenges and instead of falling down, rose up and stood stronger than ever. I am blessed to be part of such a strong, compassionate, and loving family. It is their encouragement, love, and support that has pushed me to follow my dreams and aim for the stars.

In loving memory of Michael Burgess, Jeffery Burgess, and Luke Burgess.

ACKNOWLEDGEMENTS

I would like to thank all of the professors and staff members at Ferris State University that have helped me grow personally and academically throughout my undergraduate and graduate years. I would like to specially thank Professor Jim Furstenberg and Professor Vel Pavlov who have taken the time out of their busy schedules to assist me with academic challenges and prepare me for the future. Their words of encouragement and lessons learned have helped me succeed academically and professionally. I would also like to thank my proofreader, Shawn Traynor.

Table of Contents

List of Tables	9
Abstract	11
Chapter 1: Introduction	12
Introduction.....	12
Background	13
Statement of the Problem.....	14
Purpose of the Study	15
Rationale	15
Research Questions	16
Nature of the Study	16
Significance of the Study	17
Definition of Terms.....	17
Assumptions.....	22
Limitations	23
Chapter 2: Literature Review	26
Mobile Devices	26
mHealth Applications	27
Headache Disorders	28
mHealth Applications for Headache Disorders	30

Privacy and Security Risks of mHealth Applications for Headache Disorders	31
Lack of Consumer Awareness	32
mHealth Applications Lie Outside HIPAA Regulations	32
Application Developers Ignore Current Guidelines and Regulations.....	33
Privacy Risks of mHealth Applications for Headache Disorders.....	34
Security Risks of mHealth Applications for Headache Disorders.....	35
Medical Data Interest Among Cybercriminals	36
Mobile Device Security Measures for Consumers	37
Chapter 3: Methodology	40
Description of Methodology.....	40
Design of the Study.....	41
Research Question One.....	41
Research Question Two	46
Research Question Three	47
Data Analysis	48
Research Question One.....	48
Research Question Two	52
Research Question Three	58
Chapter 4: Results.....	59
Research Question One.....	59

RISKS OF THE TOP MHEALTH APPLICATIONS FOR HD	7
Privacy and Security Risks	60
Severity of the Privacy and Security Risks.....	63
Research Question Two	64
Android	65
Top Android mHealth Applications for Headache Disorders.....	65
Non-Exclusive Top Android mHealth Applications for Headache Disorders.....	68
Exclusive Top Android mHealth Applications for Headache Disorders.....	71
iOS	73
Top iOS mHealth Applications for Headache Disorders.....	73
Non-Exclusive Top iOS mHealth Applications for Headache Disorders.....	76
Exclusive Top iOS mHealth Applications for Headache Disorders	79
Summary.....	82
Research Question Three	83
Chapter 5: Analysis and Suggestions for Further Study.....	86
Summary of Findings.....	86
Research Question 1	86
Research Question 2	86
Research Question 3	87
Comparison to Previous Studies	88
Conclusion	88

RISKS OF THE TOP MHEALTH APPLICATIONS FOR HD	8
Suggestions for Further Study	89
References.....	91
Appendix A: OWASP Mobile Top 10 Risks.....	100

List of Tables

Table 1 Mobile Device Security Measures to Protect Personal and Medical Data	38
Table 2 Top mHealth Applications for HD Comparison Results Template.....	50
Table 3 Risk Analysis Key	51
Table 4 Severity Scale	52
Table 5 Top Android mHealth Applications for HD Comparison Results Template.....	54
Table 6 Top iOS mHealth Applications for HD Comparison Results Template.....	55
Table 7 Non-Exclusive Top Android/iOS mHealth Applications for HD Comparison Results Template	56
Table 8 Exclusive Top Android mHealth Applications for HD Comparison Results Template..	57
Table 9 Exclusive Top iOS mHealth Application for HD Comparison Results Template	57
Table 10 Top mHealth Applications for HD Comparison Results	59
Table 11 Total Number of Risks for the Top mHealth Applications for HD	63
Table 12 Top Risks for the Top mHealth Applications for HD	64
Table 13 Bottom Risks for the Top mHealth Applications for HD	64
Table 14 Top Android mHealth Applications for HD Comparison Results.....	65
Table 15 Total Number of Risks for the Top Android mHealth Applications for HD.....	66
Table 16 Top Risks for the Top Android mHealth Applications for HD	67
Table 17 Bottom Risks for the Top Android mHealth Applications for HD.....	68
Table 18 Non-Exclusive Top Android mHealth Applications for HD Comparison Results.....	68
Table 19 Number of Risks for the Non-Exclusive Top Android mHealth Applications for HD .	69
Table 20 Top Risks for the Non-Exclusive Top Android mHealth Applications for HD	70
Table 21 Bottom Risks for the Non-Exclusive Top Android mHealth Applications for HD.....	70

RISKS OF THE TOP MHEALTH APPLICATIONS FOR HD	10
Table 22 Exclusive Top Android mHealth Applications for HD Comparison Results	71
Table 23 Number of Risks for the Exclusive Top Android mHealth Applications for HD	72
Table 24 Top Risks for the Exclusive Top Android mHealth Applications for HD	72
Table 25 Bottom Risks for the Exclusive Top Android mHealth Applications for HD.....	73
Table 26 Top iOS mHealth Applications for HD Comparison Results.....	74
Table 27 Number of Risks for the Top iOS mHealth Applications for HD	75
Table 28 Top Risks for the Top iOS mHealth Applications for HD	76
Table 29 Bottom Risks for the Top iOS mHealth Applications for HD.....	76
Table 30 Non-Exclusive Top iOS mHealth Applications for HD Comparison Results.....	77
Table 31 Number of Risks for the Non-Exclusive Top iOS mHealth Applications for HD	78
Table 32 Top Risks for the Non-Exclusive Top iOS mHealth Applications for HD	79
Table 33 Bottom Risks for the Non-Exclusive Top iOS mHealth Applications for HD.....	79
Table 34 Exclusive Top iOS mHealth Applications for HD Comparison Results.....	80
Table 35 Number of Risks for the Exclusive Top iOS mHealth Applications for HD	81
Table 36 Top Risks for the Exclusive Top iOS mHealth Applications for HD	81
Table 37 Bottom Risks for the Exclusive Top iOS mHealth Applications for HD.....	82
Table 38 Average Severities of the Three Android and iOS Studies	83
Table 39 Recommendations for Improving Privacy and Security of Personal and Medical Data	84

Abstract

Millions of consumers suffer from headache disorders that result in billions of dollars in lost productivity a year due to their inability to function and work normally during an episode. Headache disorders are often undiagnosed and undertreated, resulting in half of all sufferers not seeking medical attention. mHealth applications for headache disorders continue to gain popularity as consumers seek to better manage their disorder and reduce the frequency of their episodes by logging episodes, monitoring possible triggers, and managing their medication intake. Despite their advantages, mHealth applications for headache disorders may contain features that pose as a risk to the privacy and security of personal and medical data. This study involves a literature review and a comparative risk analysis of the top mHealth applications for headache disorders on the Android and iOS mobile platforms to determine what privacy and security risks exist within these applications and their severity. The results of this study can assist consumers in making better informed decisions when downloading and using these applications and can assist application developers in creating more secure mHealth applications for headache disorders.

Keywords: mHealth, Applications, Headache Disorders, Privacy, Security, Risks, Android, iOS

Chapter 1: Introduction

Introduction

Today, society is always on and always connected, as smartphones become integrated into individual's daily lives (Johnson, Levinson, & Stackpole, 2011). In 2017, over three-quarters of adults in the United States owned a smartphone (Perrin & Rainie, 2017). The reduction in the price of smartphones and the portability of these devices has contributed to their popularity over traditional devices, such as personal computers and landline phones (Al-Zarouni, 2006; Johnson, Levinson, & Stackpole, 2011). Smartphones consist of various features that were not available on traditional landlines and mobile phones, such as: cameras and sensors for location, acceleration, audio, and orientation (Dehling, Mandl, Sunyaev, & Taylor, 2015).

Smartphones allow for the use of a variety of applications at the consumer's desire, which were not available on traditional landline and mobile phones. Among the most popular type of applications today include mobile health applications, or more commonly referred to as mHealth applications (MCOL, 2015). mHealth applications assist consumers in monitoring and managing their health and can greatly improve medical services, reduce medical costs, and ultimately provide better patient care (Adhikari, Richards, & Scott, 2014; Flaherty, 2014). In 2017, approximately 1.7 billion consumers used one or more of the 325,000 mHealth applications currently available in application stores (Aspinall & Knorr, 2015; Pohl, 2017). The most popular application stores include the Apple App Store and Google Play Store, which contain nearly an equal number of mHealth applications and significantly outnumber other popular application stores (Pohl, 2017).

mHealth application developers are devoting their efforts to creating mHealth applications for chronic diseases, such as headache disorders (Baum, 2015). Consumers with headache disorders often experience high costs for medical services and limited care and as a result, most sufferers do not seek medical care (Migraine Research Foundation, 2017). Headache disorders are among the most

poorly understood and under diagnosed chronic illnesses in the world (Migraine Research Foundation, 2017). Over ten million headache disorder sufferers downloaded a mHealth application for headache disorders in 2016 (Ireland, 2017). Migraines affect over a billion individuals worldwide and is the third most prevalent illness in the world (Migraine Research Foundation, 2017). Migraines are the sixth most disabling illness in the world and 90 percent of sufferers are unable to work or function normally during an episode, which accounts for a significant amount of lack of productivity and missed days among employees (Migraine Research Foundation, 2017). By using mHealth applications for headache disorders, headache disorder sufferers can better manage their condition and overall improve their health (Ireland, 2017). mHealth applications for headache disorders can assist consumers in managing their medication intake to prevent overdosing, monitor risk factors, determine triggers for episodes, and prevent the condition from becoming chronic (Ireland, 2017).

Background

Medical data is one of the most sensitive types of information, which makes it a top target for cybercriminals (Kehoe, 2016; Aspinall & Knorr, 2015). Cybercriminals can sell medical data on the black market for up to \$500 (Kehoe, 2016). Over 80 percent of cyberattacks occur within the application, resulting in approximately eight million medical records to be stolen each year (Kehoe, 2016; Aspinall & Knorr, 2015). A lack of consumer awareness contributes to these cyberattacks, as over 80 percent of consumers believe that the mHealth applications they are using are secure and of these consumers, 60 percent believe that application developers are doing everything they can to protect their personal and medical data (Driver, 2016).

mHealth applications, including those for headache disorders, are not protected by the Health Insurance Portability and Accountability Act (HIPAA), which provides regulations for the privacy and security of consumers' medical data (Gunter, He, Nahrstedt, & Naveed, 2014). The Food and Drug Administration (FDA) does provide guidelines for the privacy and security of

medical data, but only for a significantly small portion of mHealth applications that qualify as mobile medical devices or pose significant risks (Brewer, Buller, Dellavalle, Kamel-Boulos, & Karimkhani, 2014). However, these regulations do not describe what classifies as “significant risks” and what mHealth applications fall under this stipulation (Brewer, Buller, Dellavalle, Kamel-Boulos, & Karimkhani, 2014). In addition, these regulations do not address key vulnerabilities, such as reverse-engineering, repackaging, republishing, and runtime attacks (Brewer, Buller, Dellavalle, Kamel-Boulos, & Karimkhani, 2014). Other government organizations, such as the American Telemedicine Association (ATA) and the Federal Trade Commission (FTC), have also created guidelines for the privacy and security of medical data within mHealth applications, but have had limited success as application developers desire to focus on releasing applications quickly and implementing functionality and usability over privacy and security (Kayl, Luxton, & Mishkind, 2012; Martinez-Perez & Torre-Diez, 2015; Dehling, Mandl, Sunyaev, & Taylor, 2015). In addition, complying with regulations can be extremely costly for application developers (Flaherty, 2014).

Statement of the Problem

mHealth applications for headache disorders pose significant risks to the privacy and security of consumers’ personal and medical data, as consumers are required to enter their personal and medical information into these applications in order to yield accurate results and obtain the benefits of using these applications (Adhikari, Richards, & Scott, 2014; Dehling, Mandl, Sunyaev, & Taylor, 2015). Most application developers do not follow the guidelines provided by several government organizations regarding privacy and security, as functionality and usability are desired over privacy and security to increase consumer satisfaction and gain popularity (Martinez-Perez & Torre-Diez, 2015). The lack of privacy and security requirements for mHealth applications for

headache disorders often leaves the consumer's personal and medical data to be stored and transmitted in an unencrypted state (Flaherty, 2014). The unencrypted personal and medical data makes mHealth applications for headache disorders an ideal and easy target for cybercriminals and leaves the consumer's personal and medical data vulnerable to altering and theft (Flaherty, 2014). In addition, cybercriminals can use the unsecure mHealth applications for headache disorders to gain unauthorized access to the consumer's smartphone, posing a risk to other potentially sensitive data stored on the device. Maintaining the confidentiality, integrity, and availability of the consumer's personal and medical data is critical to their health and well-being (Adhikari, Richards, & Scott, 2014). Therefore, the problem addressed in this study is the privacy and security of personal and medical data within mHealth applications for headache disorders.

Purpose of the Study

The purpose of this study is to discover what privacy and security risks exist and their severity within the top mHealth applications for headache disorders. By focusing on the sub-category of headache disorders within mHealth applications, the author can more accurately identify privacy and security risks and their severity. The objectives of this study are to compare features of mHealth applications for headache disorders that often pose as a privacy and security risk to personal and medical data and to compare mHealth applications for headache disorders on the Android and iOS mobile platforms.

Rationale

The lack of privacy and security requirements for mHealth applications for headache disorders often leaves the consumer's personal and medical data to be stored and transmitted in an unencrypted state (Flaherty, 2014). Application developers are not required to follow the guidelines provided by several government organizations regarding privacy and security, as

functionality and usability are desired over privacy and security to increase consumer satisfaction and gain popularity (Adhikari, Richards, & Scott, 2014). In order to protect the consumer's personal and medical data, it is critical for application developers to properly implement privacy and security measures within their mHealth applications for headache disorders. The results of the study will determine what privacy and security risks exist within the top mHealth applications for headache disorders and the severity of these risks. In addition, the results of this study will determine which mobile platform has the most severe privacy and security risks within their mHealth applications for headache disorders. The results of this study will provide application developers with an understanding of what privacy and security risks exist in order to gain a better understanding of the importance of implementing proper privacy and security features into their applications. Lastly, the results of this study will provide consumers with the knowledge of what privacy and security risks exist in order to be cautious and make more educated decisions when downloading and using these applications.

Research Questions

1. What privacy and security risks exist within the top mHealth applications for headache disorders and what is their severity?
2. Which mobile platform has the most severe privacy and security risks within their top mHealth applications for headache disorders?
3. What recommendations can be made to improve the privacy and security of personal and medical data within mHealth applications for headache disorders?

Nature of the Study

This study will use a quantitative, descriptive, cross-sectional approach in order to answer the research questions. Despite the popularity of mHealth applications, limited studies have been

performed in the past four years regarding the privacy and security risks within these applications. Further research is warranted to determine whether privacy and security risks are still prevalent within the mHealth applications that are popular today and if the severity of these risks remain as significant as they were four years ago. To the best of the author's knowledge, this study is the first study regarding the privacy and security risks of mHealth applications for headache disorders. Therefore, this study will serve to address the gap in research and contribute to the existing body of knowledge in the privacy and security risks of mHealth applications.

Significance of the Study

By understanding what privacy and security risks exist within mHealth applications for headache disorders and their severity, consumers can gain awareness of the risks within these applications and can be cautious and make more educated decisions when downloading and using them. In addition, government organizations can gain awareness of the severity of these risks and the importance of creating regulations for the privacy and security of consumers' personal and medical data within mHealth applications for headache disorders. Application developers can also use this knowledge to improve the privacy and security measures within their own mHealth applications for headache disorders.

Definition of Terms

Android. An operating system for smartphones and other devices, developed by Android, Inc. and later purchased by Google. The Android platform is based on the Linux operating system. (BusinessDictionary.com, n.d.-a).

Apple iOS. A mobile operating software developed by Apple and exclusively for Apple hardware. The Apple iOS operating system powers Apple's iPhone, iPad, iPod Touch, and Apple TV (BusinessDictionary.com, n.d.-b).

Application. A software program that is designed to perform a specific function directly for the consumer or, in some cases, for another application program (Rouse, 2011).

Application Developer. An individual who creates a software application (PC Magazine, n.d.).

Application Store. An online portal through which applications are made available for consumers to download. All major mobile operating system vendors, including Apple, Google, BlackBerry and Microsoft, run their own application stores, which gives them control over the software available on their respective platforms (Rouse & Steele, 2013).

American Telemedicine Association (ATA). A non-profit organization that strives to promote telemedicine and access to medical care for consumers (medical care delivered through the use of telecommunications technology) (Rouse, 2012).

Authentication. A process that ensures and confirms a consumer's identity that begins when a consumer tries to access an application or personal and medical information (Techopedia, n.d.-c)."

Availability. It ensures reliability and timely access to personal and medical data to authorized consumers (Harris, 2013).

Black Market. An illegal traffic or trade of personal and medical data (Oxford Dictionaries, n.d.).

Cloud Storage. Personal and medical data that is stored on remote servers and accessed from the Internet. It is maintained, operated, and managed by a cloud storage service provider on a server that is built on virtualization techniques (Techopedia, n.d.-d).

Confidentiality. It ensures that the necessary level of secrecy is enforced at each junction of data processing and prevents unauthorized disclosure of personal and medical data (Harris, 2013).

Cyberattack. An attempt to damage, disrupt, or gain unauthorized access to a mobile device and the personal and medical data it may contain (Dictionary.com, n.d.).”

Cybercriminal. Individuals that use technology to commit malicious activities on mobile devices with the intent of stealing sensitive personal and medical data to generate a profit (Trend Micro, n.d.).

Data. Personal and medical information that has been translated into a form that is efficient for movement or processing (Rouse & Vaughan, 2017).

Data At-Rest. Personal and medical data that is not actively moving from device to device or network to network, such as data stored on the cloud or mobile device (Lord, 2016).

Data In-Motion. Personal and medical data that is actively moving from one location to another, such as across the internet or through a private network (Lord, 2016).

Database. A collection of personal and medical information that is organized so that it can be easily accessed, managed, and updated (Hughes, Leake, & Rouse, 2017).

Feature. A notable property of a mobile device or mHealth application (Webopedia, n.d.).

Food and Drug Administration (FDA). “An agency within the U.S. Department of Health and Human Services (HHS) that oversees the manufacturing and distribution of food, pharmaceuticals, medical devices, tobacco and other consumer products and veterinary medicine (Rouse & Sutner, 2016).”

Federal Trade Commission (FTC). “A United States federal regulatory agency designed to monitor and prevent anticompetitive, deceptive or unfair business practices (Cole & Margaret, 2016).”

Global Positioning System (GPS). A “constellation” of approximately 30 well-spaced satellites that orbit the Earth and make it possible for consumers with mobile devices to pinpoint their geographic location (Peleg & Rouse, 2016).

Guideline. A document that suggests how to implement privacy and security measures in order to protect personal and medical data within mHealth applications (Cambridge Dictionary, n.d.).

Headache Disorder. A reoccurring headache that is among one of the most common disorders of the nervous system. The disorder includes, but is not limited to: migraines, tension-type headaches, and cluster headaches (World Health Organization, 2016).

Health Insurance Portability and Accountability Act (HIPAA). “A United States law designed to provide privacy standards to protect patients’ medical records and other health information provided to health plans, doctors, hospitals and other medical providers (MedicineNet.com, n.d.).”

Integrity. The assurance of the accuracy and reliability of personal and medical data that is provided and any unauthorized modifications is prevented (Harris, 2013).

Medical Data. Data that is related to medical. See definition of data.

mHealth. The use of mobile devices to improve medical outcomes, medical care services, and medical research (National Institutes of Health, 2018).

Migraine. “A condition marked by recurring moderate to severe headache with throbbing pain that usually lasts from four hours to three days, typically begins on one side of the head, but

may spread to both sides, is often accompanied by nausea, vomiting, and sensitivity to light or sound, and is sometimes preceded by an aura and is often followed by fatigue (Merriam-Webster, 2018).”

Mobile Device. A smartphone, tablet, or other similar device that is made for portability, and is therefore both compact and lightweight (Techopedia, n.d.-a).

Mobile Platform. An operating system that is specifically designed to run on mobile devices such as smartphones, tablet computers, and other handheld devices (Beal, n.d.).

Open Web Application Security Project (OWASP). “An organization that provides unbiased and practical, cost-effective information about computer and internet applications (Rouse, 2006).”

Privacy. The amount of control a consumer should be able to have, as it relates to the release of their own sensitive personal and medical information (Harris, 2013).

Privacy Policy. A document that details what personal and medical information is collected from consumers, how it will be used, and how to keep it private (Engel, 2018).

Regulatory Compliance. The process of implementing measures necessary to comply with the regulations, laws, and guidelines that govern the privacy and security of personal and medical data within mHealth applications (Safeopedia, n.d.).

Repackaging. The process of creating a customized application using an already fully functional application for malicious purposes (Symantec, 2009).

Reverse Engineering. Taking apart an application to see how it works in order to duplicate or exploit the application itself (Crawford & Rouse, 2007).

Risk. The potential for loss, damage, or destruction of personal and medical data as a result of a threat exploiting a vulnerability related to mHealth application features (Threat Analysis Group, 2010).

Security. “The defense of personal and medical data against internal and external, malicious and accidental threats. This defense includes detection, prevention, and response to threats through the use of security policies, software tools, and IT services (Bacon & Rouse, Security, 2017).”

Smartphone. A cellular telephone with an integrated computer and other features not originally associated with telephones, such as an operating system, web browsing, and the ability to run software applications, such as mHealth applications (Rouse, 2007).

Social Engineering Attacks. “An attack vector that relies heavily on human interaction and often involves tricking people into breaking normal security procedures (Bacon & Rouse, 2016).”

Social Media. Primarily internet or smartphone-based applications and tools to share information among people. Social media includes popular networking websites, like Facebook and Twitter (BusinessDictionary.com, n.d.-c).

Unauthorized Access. Viewing private accounts, messages, files, or resources that contain personal and medical data, when an individual has not been given permission from the owner to do so (BusinessDictionary.com, n.d.-d).

Vulnerability. A flaw in a mHealth application feature that can leave it open to a cyberattack (Techopedia, n.d.-b). See definition of cyberattack.

Assumptions

- Adequate and reliable research will be available and analyzed for this study.

- Experts within the research field will be available to provide additional knowledge and resources as needed during this study.
- The mHealth applications for headache disorders that were chosen for this study will be available within the appropriate application stores for download and use.
- The Android and Apple iOS smartphones used in this study will be available and function properly.
- A wireless internet connection or cellular data will be available to download and use the mHealth applications for headache disorders for this study.
- The emphasis of this study is on the privacy and security risks that exist within mHealth applications for headache disorders and not on the applications themselves.

Limitations

- The study will be completed in 2018 and is limited to the resources and information that is available at the time of the study.
- The study is limited to a 14-week period in which it must be completed.
- The study is limited to focusing on headache disorder applications which is a sub-category of mHealth applications.
- This study is limited to the top mHealth applications for headache disorders at the time of this study that were determined by performing a literature review.
- The study is limited to the features determined by the author to pose a risk to the privacy and security of personal and medical data.
- The study is limited to the Google Android and Apple iOS mobile platforms.
- The study is limited to using a Samsung Galaxy S7 and Apple iPhone 5S.

- The study is limited to using Android 7.0 (Nougat) on the Samsung Galaxy S7 and Apple iOS 11 on the iPhone 5S; which are the current versions at the time of this study.
- The study is limited to using the Google Play Store and Apple App Store to download the top mHealth applications for headache disorders.
- The study is limited to the current versions of the selected nine Android mHealth applications for headache disorders from the Google Play Store at the time of this study:
 - Acupressure: Heal Yourself (v 3.0)
 - Headache Log (v 1.32)
 - iMigraine (v 1.5)
 - Manage Your Pain Pro (v 2.692)
 - Migraine Buddy (v 24.3.4)
 - Migraine Diary (v 1.0.2)
 - Migraine eDiary (v 2.2)
 - Migraine Relief Hypnosis (v 2.23)
 - Relax Melodies (v 6.7.4)
- The study is limited to the current versions of the selected eleven iOS mHealth applications for headache disorders from the Apple App Store at the time of this study:
 - Acupressure: Heal Yourself (v 3.5)
 - Brainwave Tuner (v 4.7.1)
 - Curelator (v 1.5.8)
 - Headache Diary (v 1.8.5)
 - iHeadache (v 2.5)
 - iMigraine (v 2.0)

- Migraine Buddy (v 24.3.3)
- Migraine Coach (v 2.2.5)
- Migraine eDiary (v 2.1)
- Migraine Relief Hypnosis (v 3.11)
- Relax Melodies (v 6.2)

Chapter 2: Literature Review

Mobile Devices

The use of traditional Internet-based devices, such as desktop and laptop computers have dramatically declined in the past few years as we move towards a more mobile-oriented world. A study performed by Pew Research Center (2018) determined that 95 percent of individuals in the United States own a cell phone and of those individuals, over three-quarters own a smartphone. Heisler (2016) stated that more individuals are accessing the Internet from mobile devices than desktop or laptop computers. Pew Research Center (2018) backed this finding by stating that one in ten individuals in the United States are “smartphone only” Internet users.

Brewer, Buller, Dellavalle, Kamel-Boulos, and Karimkhan (2014) stated that the always-on, always-connected, and highly portable aspects of mobile devices have significantly contributed to their growing popularity. Mobile devices allow individuals to communicate with others in real-time and on-demand, as well as provide easier access to faster and more reliable Internet than ever before, also stated Brewer et al. (2014). According to Brewer et al. (2014), mobile devices are highly customizable, allowing individuals to adjust settings and features to meet their personal preferences and needs. Individuals are becoming increasingly reliant on mobile devices to perform both work and personal tasks. According to Meyer (2017), individuals in the United States spend an average of ten hours per day on mobile devices, which is approximately five hundred hours per year.

According to Dehling, Mandl, Sunyaev, and Taylor (2015), the most popular mobile device platforms today are Google’s Android and Apple’s iOS. comScore, Inc. (2017) confirmed this by stating that in the United States, Android consists of over 53 percent of the mobile device market

share with iOS consisting of nearly 45 percent. In total, Android and iOS consist of over 98 percent of the total mobile device market share, stated comScore, Inc (2017).

mHealth Applications

Mobile devices contain a variety of applications that are similar to programs on a traditional desktop or laptop computer. Aspinall and Knorr (2015) stated that among the most popular and rapidly growing categories of applications are mobile health applications, also known as mHealth applications. Aspinall and Knorr (2015) discovered that mHealth applications can help consumers monitor and manage their health and the data collected from these applications can assist medical professionals to provide more accurate care and ultimately leading to improved service and reduced costs. Flaherty (2014) added that mHealth applications can improve doctor-patient communication, increase access to medical care, and reduce the hospital readmissions. There is a diverse variety of mHealth applications that can be used to track an individual's heart rate, blood pressure, glucose, sleep patterns, mood, food and water intake, exercise, and provide them with medication reminders, according to Aspinall and Knorr (2015). In order to provide all the features that are desired by consumers, mHealth applications leverage a wide variety of mobile device hardware and software, including: cameras and sensors for location, acceleration, audio, and orientation; in order to collect and store consumer-reported personal and medical data, according to Dehling, Gao, Schneider, and Suryaev (2015).

As previously confirmed, Google's Android and Apple's iOS consist of the majority of the mobile device market share. The associated application stores for these platforms are the Google Play Store and Apple App Store. A study performed by Martinez-Perez and Torre-Diez (2015) showed that in 2012 there were approximately 40,000 mHealth applications. Five years later, in

2017, Pohl (2017) conducted a study which showed that there was more than 325,000 mHealth applications available in these popular application stores.

Over 60 percent of consumers who own a smartphone have downloaded at least one mHealth application, according to MCOL (2015). In a 2015 study performed by Kehoe (2016), more than three billion mHealth applications were downloaded in popular application stores.

In 2017, Android surpassed iOS in the amount of mHealth applications available in its application store making Android the leading mHealth platform, according to Pohl (2017). A study performed by Pohl (2017), showed that the Google Play Store saw a dramatic spike of mHealth applications released in 2017 with a 50 percent increase in the amount of these applications, which was the highest growth among all application stores. Other application stores, include: Windows Phone, Amazon Application Store, and Blackberry World, according to Pohl (2017). However, application developers are focusing on creating mHealth applications for the Google Play Store and Apple App Store in order to provide a serious outreach to consumers as these application stores are the most popular and have a nearly equal amount of mHealth applications already available, stated Pohl (2017).

Headache Disorders

The World Health Organization (2016) described a headache disorder as a headache that is recurring and is the most common disorder in the nervous system. The World Health Organization (2016) stated that the type of conditions that are considered headache disorders includes recurring and severe: migraines, tension headaches, and cluster headaches. Migraines are the primary headache disorder, according to the World Health Organization (2016). The Migraine Research Foundation (2017) described a migraine as a severe headache that includes other symptoms, such as: visual disturbances, nausea, vomiting, dizziness, extreme sensitivity to sound,

light, touch, and smell, and tingling or numbness in the extremities or face. The cause of migraines is unknown, according to McCarthy (2017). However, McCarthy (2017) explained that a number of triggers can lead to a migraine, including: bright lights, stress, tiredness, medications, and certain types of foods. McCarty (2017) stated that hormone fluctuations, family history, gender, and age can increase an individual's risk of migraines, but migraines are often treated with medication.

A study conducted by the Migraine Research Foundation (2017) discovered that 39 million individuals in the United States suffer from migraines, naming migraines as the third most prevalent illness and sixth most disabling illness in the world. Ninety percent of migraine sufferers are unable to work or function normally during an episode resulting in \$36 billion in lost productivity each year in the United States, according to the Migraine Research Foundation (2017). Those individuals that suffer from chronic migraines experience an episode at least fifteen times per month, according to the Migraine Research Foundation (2017).

The Migraine Research Foundation (2017) stresses that migraines are often undiagnosed and undertreated as over half of all migraine sufferers are never diagnosed. Those that suffer from migraines often receive high costs for medical care and are limited to the amount of quality care that they receive, resulting in many sufferers not seeking medical attention for their migraines, according to the Migraine Research Foundation (2017). Those individuals that are able to seek medical attention and are prescribed medication often suffer from medication overuse increasing the amount of migraine episodes they receive, as discovered by the Migraine Research Foundation (2017).

mHealth Applications for Headache Disorders

Individuals who suffer from a chronic condition, such as headache disorders, are the most common target audience for mHealth application developers, according to Baum (2015). A study performed by Ireland (2017) found that ten million migraine sufferers downloaded a mHealth application, including those for headache disorders, in 2016. Ireland (2017) stated that even though medication can be used to treat the symptoms of a migraine, migraine sufferers need to manage their medication intake and monitor triggers to be able to effectively reduce the amount of migraines they receive and prevent their condition from becoming chronic. Ireland (2017) stated that mHealth applications for headache disorders can assist migraine sufferers in performing these tasks by providing them with a variety of features that may include:

- Logbooks or diaries; recording the migraine episodes, including time, duration, possible triggers, and symptoms to better understand their condition and communicate with medical professionals.
- Information repository and coaching; provides the migraine sufferer with information about their disorder and best methods for identifying, treating, and managing their disorder in order to prevent or reduce the frequency of their episodes.
- Pattern recognition; analyzing the user-provided data on their migraine episodes in order to alert the consumer of possible triggers.
- Sensors; using the weather conditions and user-provided data to determine if and how weather influences the occurrence and frequency of their episodes.
- Data operability; allows the consumer to transfer personal and medical data to and from the application as needed and create a report for personal record and sharing with medical professionals.

Privacy and Security Risks of mHealth Applications for Headache Disorders

mHealth applications, including those for headache disorders, were predicted to rapidly gain popularity and bring a significant change to the medical industry, however despite their growing popularity mHealth applications have not made the impact that Fogg (2014) and many other researchers predicted. While mHealth applications, including those for headache disorders, are an ideal tool for many consumers to monitor and track medical conditions, mHealth application features pose a number of privacy and security risks, according to Aspinall and Knorr (2015). The privacy and security risks that exist within mHealth applications, including those for headache disorders, pose as a significant risk to the confidentiality, integrity, and availability of consumers' personal and medical data. In order to maximize the benefits of mHealth applications, including those for headache disorders, consumers are required to reveal their personal and medical information, according to Dehling, Gao, et al. (2015).

Medical professionals have been slow to prescribe mHealth applications, including those for headache disorders, due to the lack of trustworthiness, according to Fogg (2014). Adhikari, Richards, and Scott (2014) explained that if the integrity of the consumer's personal and medical data is compromised, it may cause harm to consumers as they rely on these applications to help treat their medical conditions and may delay seeking the proper care. O'Reilly (2017) stressed that mHealth applications, including those for headache disorders, have the ability to provide revolutionizing medical care to consumers, however the future of these applications and medical care depends on ensuring the safety and security of electronic personal and medical data. In order to gain the trust of consumers and medical providers, application developers must first become aware of the privacy and security risks that exist within mHealth applications, including those for headache disorders, in order to improve their own applications.

The following sections contain several privacy and security risks that may relate to other sub-categories of mHealth applications or mHealth applications in general, however are privacy and security risks that may directly impact mHealth applications for headache disorders.

Lack of Consumer Awareness. In a study performed by Kehoe (2016), 87 percent of consumers believed that their mHealth applications, including those for headache disorders, were “adequately secure” and 75 percent believed that the application developers were doing “everything they can” to protect their mHealth applications and personal and medical data. However, Kehoe (2016) stated that nearly half of consumers believed that their mHealth application, including those for headache disorders, would be hacked within the next six months. Although, a study by Driver (2016) showed that 80 percent of consumers would stop using and change mHealth applications, including those for headache disorders, if they knew their mHealth applications were not secure. By gaining awareness of the privacy and security risks that exist within mHealth applications, including those for headache disorders, consumers can make better decisions when downloading and using these applications and push application developers to better secure their own mHealth applications.

mHealth Applications Lie Outside HIPAA Regulations. As the medical industry has shifted towards intangible, electronic medical data in recent years, many privacy and security regulations have been created to protect the confidentiality, availability, and integrity of consumers medical data, such as the Health Insurance Portability and Accountability Act (HIPAA). However, the requirements to be HIPAA-compliant only applies to medical facilities, insurance companies, and doctors, and does not apply to mHealth applications, including those for headache disorders, according to Aspinall and Knorr (2015). Gunter, He, Nahrstedt, and Naveed (2014) explained that the medical data used within mHealth applications, including those for headache disorders, is as

sensitive as the medical data used by HIPAA-compliant entities. Therefore, the medical data used within mHealth applications, including those for headache disorders, should be treated with the same level of sensitivity as the medical data used by HIPAA-compliant entities, stated Gunter et al. (2014). However, since mHealth applications, including those for headache disorders, are not regulated by HIPAA, application developers are free to handle medical data used within their mHealth applications as desired, according to Gunter et al. (2014).

Application Developers Ignore Current Guidelines and Regulations. Application developers are responsible for keeping consumer personal and medical data within their mHealth applications secure, however they often choose functionality and usability over privacy and security as they seek to be the first to develop and release new applications, according to Martinez-Perez and Torre-Diez (2015).

Many organizations have created guidelines for application developers to better ensure the privacy and security of personal and medical data used within their mHealth applications; including those for headache disorders. Kayl, Luxton, and Mishkind (2012) stated that the American Telemedicine Association (ATA) created guidelines for the privacy and security of personal and medical data, that are similar to those of HIPAA, but geared towards mHealth applications; including those for headache disorders. In addition, the Federal Trade Commission (FTC) created recommendations for the privacy policies of mHealth applications, including those for headache disorders, according to Dehling, Mandl, et al. (2015).

One of the top contributors in providing guidelines for mHealth applications, including those for headache disorders, is the United States Food and Drug Administration (FDA). According to Misra (2014), the FDA provides regulatory oversight for mHealth applications that, if compromised, pose a risk to consumer safety. However, the FDA only regulates a small portion

of mHealth applications, which are classified as “mobile medical devices”, according to Aspinall and Knorr (2015). Aspinall and Knorr (2015) also stated that the FDA intentionally excluded those mHealth applications “that provide or facilitate supplement clinical care, by coaching or prompting, to help patients manage their health in their daily environment.” In addition, the guidelines do not address key vulnerabilities, such as reverse-engineering, repackaging, republishing, and runtime attacks, according to Misra (2014). Flaherty (2014) explained that the guidelines do state that the FDA will regulate those mHealth applications, including those for headache disorders, that “pose significant risks”, however do not state what types of applications are included and what is classified as a “significant risk”.

According to Baum (2015), despite the fact that application developers desire to assist consumers in improving their health and reducing medical costs, privacy and security guidelines are often not implemented because these guidelines can be costly. In addition, application developers seek to implement functionality and usability over privacy and security, in order to attract consumers and increase profits as stated by Baum (2015).

Privacy Risks of mHealth Applications for Headache Disorders. Even though consumers desire control over their personal and medical data and the FTC has created guidelines for privacy policies, many application developers have failed to create a privacy policy for their mHealth applications, including those for headache disorders, according to Dehling, Mandl, et al. (2015). A study performed by Dehling, Mandl, et al. (2015) found that over 30 percent of mHealth applications, including those for headache disorders, do not contain a privacy policy and of those mHealth applications that do, 66 percent do not address the application itself. Dehling, Mandl, et al. (2015) explained that consumers should have transparency in how their personal and medical

data is being handled and allow consumers to choose a mHealth application that best fits their preferences.

Flaherty (2014) reported a study by the Privacy Rights Clearinghouse that discovered over a third of mHealth applications, including those for headache disorders, transmit unencrypted personal and medical data to advertising and data analysis companies without the consumer's knowledge or consent. Flaherty (2014) continued by stating that consumers are required to enter their personal and medical information into these applications, but are unaware of what the application developer does with this information. Flaherty (2014) explained that every mobile device has a unique number that allows companies to gather information about the consumer and create a profile that can be shared with advertisers. While consumers voluntarily share their sensitive personal and medical information and blindly trust these applications, many consumers believe that their information stays protected, according to Flaherty (2014). Application stores have the ability to remove applications that infringe on consumer privacy, however do not have specific policies for the privacy and security of medical information, according to Dehling, Mandl, et al. (2015).

Security Risks of mHealth Applications for Headache Disorders. Data security is critical for assuring privacy, allowing interoperability, and maximizing the full capabilities of mobile devices, according to Kayl et al. (2012). Kayl et al. (2012) explained that mHealth applications, including those for headache disorders, contain a large amount of sensitive personal and medical data that is required to be secure when being stored and transmitted. However, a study performed by Aspinall and Knorr (2015) showed that many mHealth applications, including those for headache disorders, do not adequately secure medical data when being stored and transmitted.

Driver (2016) found that 90 percent of mHealth applications, including those for headache disorders, that were tested during their study contained at least two of the Open Web Application Security Project (OWASP) Mobile Top 10 Risks. A similar study performed by Kehoe (2016) found that 86 percent of mHealth applications, including those for headache disorders, contain at least two of the OWASP Mobile Top 10 Risks. In the study performed by Driver (2016) it was discovered that 98 percent of mHealth applications, including those for headache disorders, did not contain binary protection that is identified as the most prevalent security vulnerability. According to Kehoe (2016), a lack of binary protection increases the risk for reverse engineering, tampering, and ultimately medical data and identity theft. Appendix A provides a list and description of each of the OWASP Mobile Top 10 Risks.

Third-party companies, such as Happtique, have attempted to evaluate and certify mHealth applications, that meet their strict security standards, however, have been suspended as significant security vulnerabilities were still discovered within the approved applications, according to Misra (2014). According to Kehoe (2016), nearly half of the companies involved in creating mHealth applications, including those for headache disorders, do not have the appropriate funds to implement data security.

Medical Data Interest Among Cybercriminals. According to Kehoe (2016), medical data is among the top targets for cybercriminals, as medical data can be sold on the black market for up to \$500. Medical data is one of the most sensitive types of data, yet a two-year study by Landi (2018) showed that in the United States alone there was over 920 breaches within the medical industry and over 30 million medical records were affected. Landi (2018) also discovered that there was an average of at least one medical data breach per day in 2017.

By exploiting the security vulnerabilities within mHealth applications, including those for headache disorders, cybercriminals can not only gain access to sensitive medical data, they can also gain unauthorized access to the mobile device, as stated by Misra (2014). When a cybercriminal gains unauthorized access to the mobile device, they also gain access to other sensitive types of information, such as: usernames, passwords, credit card information, and banking information, according to Misra (2014).

In a study performed by Misra (2014), 90 percent of the Android mHealth applications that were tested, appeared to have been hacked. Of the Android mHealth applications that appeared to be hacked, 40 percent of the applications were FDA-approved, according to Misra (2014). However, of the iOS mHealth applications that were tested during the study performed by Misra (2014), none of the applications appeared to have been hacked. It is important to note that it is unknown whether or not mHealth applications for headache disorders were included in this study, however the severity of the risks addressed in this study are important to understand when addressing the privacy and security risks of these applications.

Mobile Device Security Measures for Consumers

Consumers should demand that application developers implement privacy and security measures into their mHealth applications, including those for headache disorders, in order to protect their personal and medical data, recommended Misra (2014). Misra (2014) also recommended that consumers should be aware of the privacy and security risks of mHealth applications, including those for headache disorders, when downloading and using them. However, consumers have little control over the privacy and security measures that are implemented in mHealth applications, including those for headache disorders, but can take measures to secure their mobile device in order to better protect their personal and medical data. Table 1 summarizes the

mobile device security measures recommended by Kehoe (2016) and the U.S. Department of Health and Human Services (2013) in order to protect consumers' personal and medical data.

Table 1

Mobile Device Security Measures to Protect Personal and Medical Data

Measure	Description
Download applications only from authorized application stores.	Most authorized application stores have more rigorous security protocols in place to help ensure applications can be trusted.
Do not jailbreak or root mobile devices.	Jailbreaking or rooting devices negates critical security measures that are designed to help protect you and your data.
Use a password or other user authentication	Mobile devices can be configured to require passwords, personal identification numbers (PINs), or passcodes to gain access to it. The password, PIN, or passcode field can be masked to prevent people from seeing it. Mobile devices can also activate their screen locking after a set period of device inactivity to prevent an unauthorized user from accessing it.
Install and enable encryption	Encryption protects medical information stored on and sent by mobile devices. Mobile devices can have built-in encryption capabilities, or you can purchase and install an encryption tool on your device.
Install and activate remote wiping and/or remove disabling	Remote wiping enables you to erase data on a mobile device remotely. If you enable the remove wipe feature, you can permanently delete data stored on a lost or stolen mobile device. Remote disabling enables you to lock or completely erase data stored on a mobile device if it is lost or stolen. If the mobile device is recovered, you can unlock it.
Disable and do not install or use file sharing applications	File sharing is software or a system that allows Internet users to connect to each other and trade files. However, file sharing can also enable unauthorized users to access your mobile device without your knowledge. By disabling or not using file sharing applications, you reduce a known risk to data on your mobile device.
Install and enable a firewall	A personal firewall on a mobile device can protect against unauthorized connections. Firewalls intercept incoming and outgoing connection attempts and block or permit them based on a set of rules.
Install and enable security software	Security software can be installed to protect against malicious applications, viruses, spyware, and malware-based attacks.
Keep your security software up-to-date	When you regularly update your security software, you have the latest tools to prevent unauthorized access to medical information on or through your mobile device.

Research mobile applications before downloading	Before you download and install an application on your mobile device, verify that the application will perform only functions you approve of. Use known websites or other trusted sources that you know will give you reputable reviews on the application.
Maintain physical control	The benefits of mobile devices – portability, smart size, and convenience – are also their challenges for protecting and security medical information. Mobile devices are easily lost or stolen. You can limit the unauthorized users’ access, tampering and theft of your mobile device when you physically secure the device.
Use adequate security to send or receive medical information over public Wi-Fi networks	Public Wi-Fi networks can be an easy way for unauthorized users to intercept information. You can protect and secure medical information by not sending or receiving it when connected to a public Wi-Fi network, unless you can use secure, encrypted connections.
Delete all stored medical information before discarding or reusing the mobile device	When you use software tools that thoroughly delete (or wipe) data stored on a mobile device before discarding or reusing the device, you can protect and secure medical information from unauthorized access. HHS OCR has issued guidance that discusses the proper steps to take to remove medical information and other sensitive data stored on your mobile device before you dispose or reuse the device.

Chapter 3: Methodology

Description of Methodology

This study will use a quantitative, descriptive, cross-sectional approach in order to answer the following research questions:

- What privacy and security issues exist within the top mHealth applications for headache disorders and what is their severity?
- Which mobile platform has the most severe privacy and security risks within their top mHealth applications for headache disorders?
- What recommendations can be made to improve the privacy and security of personal and medical data within mHealth applications for headache disorders?

This study will use a structured, comparative risk analysis approach to analyze the top mHealth applications for headache disorders that were determined by performing a literature review. This study will provide a “snapshot” of the privacy and security risks that exist within the top mHealth applications for headache disorders at the time of this study. This study was limited to the versions of the top mHealth applications for headache disorders that were available from the appropriate application stores at the time of this study. This study will analyze the relationship between particular features of mHealth applications for headache disorders that may pose as a risk to the privacy and security of personal and medical data.

The results of this study will provide an understanding of the privacy and security risks that exist within the top mHealth applications for headache disorders in order to provide the consumer with the knowledge necessary to make informed decisions when downloading and using these applications. It will also provide the necessary knowledge for application developers to improve the privacy and security features within their own mHealth applications for headache

disorders. After collecting and analyzing the data, recommendations will be made for improving the privacy and security of personal and medical data within mHealth applications for headache disorders.

Design of the Study

Research Question One. In this section the following research question will be addressed, “What privacy and security issues exist within the top mHealth applications for headache disorders and what is their severity?” To address this research question, a comparative risk analysis will be performed of the top mHealth applications for headache disorders. The selection of the top mHealth applications for headache disorders was determined by performing a literature review. Axonoptics (2017), McCarthy (2017), and Oliveto (2016) provided a list of the top mHealth applications for headache disorders in 2016-2017 that will be combined to form a complete list with duplicates only being addressed once.

By performing a literature review, twelve features were identified as posing a risk to the privacy and security of personal and medical data. Since security helps protect the privacy of personal and medical data, the features were not uniquely defined as posing only a risk to privacy or security. In order to identify the privacy and security risks that exist within each of the top mHealth applications for headache disorders and determine the severity of these risks, the following risk analysis questions will be asked when analyzing each mHealth application for headache disorders. Each risk analysis question is associated with a feature within mHealth applications for headache disorders that pose as a risk to the privacy and security of personal and medical data. It is important to note that the ideal answer for the first six risk analysis questions is “no”, as these features pose as a privacy and security risk to personal and medical data. In addition,

the ideal answer for the last six risk analysis questions is “yes”, as these features increase the privacy and security of personal and medical data.

Does the mHealth application for headache disorders allow the consumer to create an account? By allowing the consumer to create an account, multiple consumers may be able to use the application on the same device. Depending on where their personal and medical data is stored, the consumer may be able to also access all of their personal and medical data from another device. However, creating an account still requires at least a small amount of the consumer’s personal and medical data to be stored on a database. This data may include their first and last name, age or date of birth, phone number, email address, height, weight, etc. Therefore, creating an account may pose as a significant risk to the privacy and security of personal and medical data.

Does the mHealth application for headache disorders store personal or medical data on the cloud or mobile device? Storing data allows the consumer to record their episodes and access details about their previous ones. It allows the mHealth application for headache disorders to determine patterns within their previous episodes in order to provide the consumer with statistics and possible triggers. However, when a mHealth application for headache disorders allows the consumer to store personal and medical data either on the cloud or locally on the mobile device, unauthorized access may occur, posing a significant risk to the privacy and security of the personal and medical data.

Does the mHealth application for headache disorders allow the consumer to export personal and medical data? When a mHealth application for headache disorders stores personal and medical data, it may contain a feature for exporting data for the consumer to use if desired. The consumer’s personal and medical data may be exported into a report and shared with medical

professionals, family, and friends, which can ultimately pose as a significant risk to the privacy and security of personal and medical data.

Does the mHealth application for headache disorders allow the use of GPS? GPS provides the consumer with the ability to track local weather conditions to determine how weather potentially triggers their migraines. In order to obtain local weather conditions, the mHealth application for headache disorders must have permission to use GPS. The use of GPS can pose as a significant risk to the privacy and security of personal and medical data. An individual who gains unauthorized access to location data can determine where the consumer is located, travel patterns, and even the consumer's identity. In addition, location data can be used to send the consumer more targeted advertisements.

Does the mHealth application for headache disorders have advertisements? Advertisements are commonly seen as an annoyance with little benefits. It is possible that advertisements may include recommendations for other similar applications or other types of applications that may be of interest to the consumer. However, advertisements are a common way to get consumers to visit a malicious website or install malicious code, in order for the cybercriminal to gain access to the consumer's personal and medical data or the consumer's mobile device itself. Advertisements are also a common way for cybercriminals to perform social engineering attacks to trick the consumer into providing personal and medical information. Ultimately, advertisements can lead to the compromise of the privacy and security of personal and medical data.

Does the mHealth application for headache disorders allow the consumer to update their account information? Providing consumers with the ability to update their account information allows for any inaccurate information that was entered when creating the account to be corrected,

as well as update information as changes occur. Ultimately, by allowing the consumer to update their account information, it increases the accuracy of personal and medical data. However, by allowing the account information to be updated, an individual that gains unauthorized access can provide false information which can lead to inaccurate conclusions and misdiagnoses.

Does the mHealth application for headache disorders require the consumer to authenticate? The advancement in mobile device technology has led to an increase in the amount of options available for consumer authentication. Common methods for authentication in today's mobile devices include username and password, PIN, pattern, fingerprint, and facial recognition. Authentication increases security by only allowing authorized consumers to access the mHealth application for headache disorders. When the mHealth application for headache disorders does not require the consumer to authenticate before using the application, the risk of unauthorized access is significantly increased and ultimately can compromise the privacy and security of the personal and medical data.

Does the mHealth application for headache disorders allow the consumer to delete their account? When the consumer desires to no longer use the mHealth application for headache disorders, it is necessary for their account and any personal and medical data to be completely and permanently deleted. If the account is not deleted when the consumer no longer desires to use the mHealth application for headache disorders, it can increase the risk of unauthorized access to their personal and medical data. Ultimately, this can compromise the privacy and security of the personal and medical data.

Does the mHealth application for headache disorders contain a privacy policy? A privacy policy contains details about what data is collected from the consumer, how it will be used, and who it will be shared with. A privacy policy can assist consumers in making informed

decisions about what mHealth applications for headache disorders to use by providing an understanding of how the privacy and security of their personal and medical data can be affected by using the mHealth application for headache disorders. When a mHealth application for headache disorders does not have a privacy policy, the consumer will not be aware of how the application developer plans to protect their personal and medical data.

Does the mHealth application for headache disorders comply with any guidelines or regulations? As previously mentioned in chapter two, several United States organizations have created guidelines or regulations for implementing privacy and security measures within mHealth applications for headache disorders in order to protect personal and medical data. When application developers do not follow the guidelines or comply with the regulations, privacy and security features may not be implemented or may not be implemented properly within the mHealth application for headache disorders. Ultimately, this can impact the privacy and security of personal and medical data.

Does the mHealth application for headache disorders require the consumer to authenticate each time they use the application? When creating the account, the mHealth application for headache disorders may require the consumer to set up a method of authentication. Once the account is created, the consumer may be automatically logged into the application and stay logged in until they log out. While it may be inconvenient for the consumer to authenticate each time they use the application, this can protect their personal and medical data from unauthorized access.

Does the mHealth application for headache disorders have a strong password policy? Passwords are one of the most common forms of authentication at the time of this study. As previously mentioned, the mHealth application for headache disorders may require the consumer

to set up a method of authentication when creating their account. Consumers often use simple and easy to remember passwords, such as “password” or “password123”. Strong and complex passwords can protect personal and medical data from unauthorized access. The following is a list of recommendations from OWASP (2013) for implementing a strong password policy:

- Password must meet at least three out of the following four complexity rules
 - At least one uppercase character (A-Z)
 - At least one lowercase character (a-z)
 - At least one digit (0-9)
 - At least one special character (punctuation); including spaces
 - At least 10 characters
 - At most 128 characters
 - Not more than two identical characters in a row (e.g. 111 is not allowed)

Research Question Two. In this section the following research question will be addressed, “Which mobile platform has the most severe privacy and security risks within their top mHealth applications for headache disorders?” To address this research question, a comparative risk analysis will be performed of the top Android and iOS mHealth applications for headache disorders. This comparative risk analysis will follow the same design as the comparative risk analysis for the first research question. As previously mentioned, the selection of the top mHealth applications for headache disorders was determined by performing a literature review. Axonoptics (2017), McCarthy (2017), and Oliveto (2016) provided a list of the top Android and iOS mHealth applications for headache disorders in 2016-2017 that will be combined to form a complete list with duplicates only being addressed once.

Similar to the first research question, a literature review was performed to identify twelve features that pose as a privacy and security risk to personal and medical data. In order to determine which mobile platform has the most severe privacy and security risks, the risk analysis questions used in the comparative risk analysis of the first research question will be used.

Three studies will be performed on the top Android and iOS mHealth application for headache disorders. The first study will consist of all the top Android and iOS mHealth applications for headache disorders, regardless of whether or not they are exclusive to each mobile platform. The second study will consist of only those top Android and iOS mHealth applications for headache disorders that are not exclusive to each mobile platform and therefore will include only those top Android and iOS mHealth applications for headache disorders that are available on both mobile platforms. The third study will consist of only those top Android and iOS mHealth applications for headache disorders that are exclusive to each mobile platform and therefore will include only those top Android and iOS mHealth applications for headache disorders that are available on only one of the platforms. The purpose of these three studies is to provide a different perspective of the top Android and iOS mHealth applications in order to accurately determine which platform has the most severe privacy and security risks.

Research Question Three. In this section the following research question will be addressed, “What recommendations can be made to improve the privacy and security of personal and medical data within mHealth applications for headache disorders?” What recommendations will be made for improving the privacy and security of personal and medical data within mHealth applications for headache disorders will be determined after the data is collected and analyzed. All data from the study will be analyzed to provide quality and accurate recommendations, however the top and bottom features that pose as a risk to the privacy and security of personal and medical

data will be the primary focus. Recommendations will be made based on the author's expertise in the field of information security. Recommendations will be made for both the consumer and application developers.

Data Analysis

Research Question One. In this section, the following research question will be addressed, "What privacy and security risks exist within the top mHealth applications for headache disorders and what is their severity?" Each of the top mHealth applications for headache disorders will be downloaded from the appropriate application store. The risk analysis questions previously provided will be asked when using each of the top mHealth application for headache disorders to determine what features pose as a privacy and security risk to personal and medical data. To record and analyze the results of the study, the template in Table 2 will be used. As previously mentioned, each of the risk analysis questions correspond with a feature within mHealth applications for headache disorders that may pose as a privacy and security risk to personal and medical data. Each of the risk analysis questions correspond with a column in Table 2. If the feature is present within the mHealth application for headache disorders and poses as a risk to the privacy and security of personal and medical data, the column will be marked with a "1". If the feature is not present within the mHealth application for headache disorders and does not pose as a risk to the privacy and security of personal and medical data, the column will be marked with a "0". If the feature is not applicable due to other features not be implemented within the mHealth application for headache disorders, the column will be marked with a "-". Table 3 provides the risk analysis key that will be used when recording the results of the study in Table 2.

The "update account information" and "delete account" features are dependent on the "create account" feature. If the mHealth application for headache disorders does not allow the

consumer to create an account, these two features will be not applicable and will not count towards the totals. The “export data”, “consumer authentication”, and “compliance” features are dependent on the “data storage” feature. If the mHealth application for headache disorders does not store personal and medical data, there will be no data to export or protect by authenticating and will not need to comply with guidelines or regulations for the privacy and security of personal and medical data. Therefore, these three features will not be applicable and will not count towards the totals. The “authenticate each use” and “password policy” features are dependent on the “consumer authenticate” feature. If the mHealth application for headache disorders does not require the consumer to authenticate, these two features will not be applicable and will not count towards the totals.

After answering all of the risk analysis questions, the total for each mHealth application for headache disorders will be calculated, as well as a percentage of risks it contains out of the total amount of applicable features. The percentages calculated for each mHealth application for headache disorders will be used to determine the overall severity for each application by using the severity scale in Table 4. The average severity will be determined by using the percentages from each mHealth application for headache disorders. It is important to note that the percentages are rounded to the nearest whole number. Any mHealth applications for headache disorders that are above the average will be noted as the most severe and will be further analyzed.

Next, the total for each particular feature of mHealth applications for headache disorders will be calculated, as well as the percentage of risks it contains out of the total amount of mHealth applications for headache disorders that are applicable. Again, the percentages and averages are rounded to the nearest whole number and any feature above the average will be noted as the most severe and will be further analyzed.

Migraine eDiary (Android)																
Migraine Relief Hypnosis (Android)																
Relax Melodies (Android)																
^s Acupressure: Heal Yourself (iOS)																
^s Brainwave Tuner (iOS)																
Curelator (iOS)																
^s Headache Diary (iOS)																
iHeadache (iOS)																
iMigraine (iOS)																
Migraine Buddy (iOS)																
Migraine Coach (iOS)																
Migraine eDiary (iOS)																
Migraine Relief Hypnosis (iOS)																
Relax Melodies (iOS)																
Total																
Total (%)																

^s Paid Application * Poses Risk if Not Present





Table 3

Risk Analysis Key

1	Risk
0	Not Risk
-	Not Applicable

Table 4

Severity Scale

	Total	Severity
	0% to 24%	Low
	25% to 49%	Medium
	50% to 74%	High
	75% to 100%	Very High

Research Question Two. In this section the following research question will be addressed, “Which mobile platform has the most severe privacy and security risks within their top mHealth applications for headache disorders?” Each of the top Android and iOS mHealth applications for headache disorders will be downloaded from the appropriate application store. The risk analysis questions previously provided will be asked when using each Android and iOS mHealth application for headache disorders in order to determine what features pose as a risk to the privacy and security of personal and medical data and ultimately what their severity is. To record and analyze the results of the study, the template in Table 5 will be used for the top Android mHealth applications for headache disorders and Table 6 will be used for the top iOS mHealth applications for headache disorders. The template in Table 7 will be used for each mobile platform to record and analyze the top mHealth applications for headache disorders that are non-exclusive and therefore found on both mobile platforms. The template in Table 8 will be used for the top exclusive Android mHealth applications for headache disorders and Table 9 will be used for the top exclusive iOS mHealth applications for headache disorders. The template in Table 8 and Table 9 will only include those top Android and iOS mHealth applications for headache disorders that are exclusive and therefore found only on one of the mobile platforms.

As previously mentioned, each of the risk analysis questions corresponds with a feature within Android and iOS mHealth applications for headache disorders that may pose as a privacy and security risk to personal and medical data. Each of the risk analysis questions correspond with a column in

Table 5 through Table 9. If the feature is present within the Android or iOS mHealth application for headache disorders and poses as a risk to the privacy and security of personal and medical data, the column will be marked with a “1”. If the feature is not present within the Android or iOS mHealth application for headache disorders and does not pose as a risk to the privacy and security of personal and medical data, the column will be marked with a “0”. If the feature is not applicable due to other features not be implemented within the Android or iOS mHealth application for headache disorders, the column will be marked with a “-” and will not count towards the totals. After answering all of the questions, the total for each Android and iOS mHealth application for headache disorders will be calculated, as well as a percentage of risks it contains out of the total amount of applicable mHealth applications for headache disorders for each mobile platform. The percentages calculated for each Android and iOS mHealth application for headache disorders will be used to determine the severity by using the severity scale in Table 4. The percentages will be used to calculate an average severity for all Android or iOS mHealth applications for headache disorders.

The percentages will also be used to determine what features pose the highest risk to the privacy and security of personal and medical data. Those with the highest percentage, or highest risk based on the severity scale in Table 4, will be included in a table of the top risks. Those with the lowest percentage, or the lowest risk based on the severity scale in Table 4, will be included in a table of the bottom risks.

After answering all of the questions, the total for each Android or iOS mHealth application for headache disorders will be calculated, as well as the percentage of risks it contains out of the total amount of applicable mHealth applications for headache disorders for each mobile platform. The percentages calculated for each Android and iOS mHealth application for headache disorders will be used to determine the overall severity for each application also using the severity scale in

Table 4. The average severity will be determined by using the percentages from each application. As a reminder, the percentages are rounded to the nearest whole number. Any Android or iOS mHealth application for headache disorders that is above the average will be noted as the most severe and will be further analyzed.

Table 5

Top Android mHealth Applications for HD Comparison Results Template

		Features														
		Create Account	Update Account Information	Data Storage	Export Data	GPS	Advertisements	* Delete Account	* Consumer Authentication	* Authenticate Each Use	* Password Policy	* Privacy Policy	* Compliance	Total	Total (%)	
Applications	[§] Acupressure: Heal Yourself															
	Headache Log															
	iMigraine															
	[§] Manage Your Pain Pro															
	Migraine Buddy															
	Migraine Diary															
	Migraine eDiary															
	Migraine Relief Hypnosis															
	Relax Melodies															
	Total															
	Total (%)															

[§] Paid Application * Poses Risk if Not Present

Table 6

Top iOS mHealth Applications for HD Comparison Results Template

	Features													
	Create Account	Update Account Information	Data Storage	Export Data	GPS	Advertisements	* Delete Account	* Consumer Authentication	* Authenticate Each Use	* Password Policy	* Privacy Policy	* Compliance	Total	Total (%)
[§] Acupressure: Heal Yourself														
[§] Brainwave Tuner														
Curelator														
[§] Headache Diary														
iHeadache														
iMigraine														
Migraine Buddy														
Migraine Coach														
Migraine eDiary														
Migraine Relief Hypnosis														
Relax Melodies														
Total														
Total (%)														

[§] Paid Application * Poses Risk if Not Present

Table 7

Non-Exclusive Top Android/iOS mHealth Applications for HD Comparison Results Template

		Features														
		Create Account	Update Account Information	Data Storage	Export Data	GPS	Advertisements	* Delete Account	* Consumer Authentication	* Authenticate Each Use	* Password Policy	* Privacy Policy	* Compliance	Total	Total (%)	
Applications	^s Acupressure: Heal Yourself															
	iMigraine															
	Migraine Buddy															
	Migraine eDiary															
	Migraine Relief Hypnosis															
	Relax Melodies															
	Total															
	Total (%)															

^s Paid Application * Poses Risk if Not Present

Applications	§ Acupressure: Heal Yourself															
	§ Brainwave Tuner															
	Curelator															
	§ Headache Diary															
	iHeadache															
	iMigraine															
	Migraine Buddy															
	Migraine Coach															
	Migraine eDiary															
	Migraine Relief Hypnosis															
	Relax Melodies															
	Total															
	Total (%)															

§ Paid Application * Poses Risk if Not Present

Research Question Three. In this section the following research question will be addressed, “What recommendations can be made to improve the privacy and security of personal and medical data within mHealth applications for headache disorders?” The recommendations for improving the privacy and security of personal and medical data within mHealth applications for headache disorders for both consumers and application developers will be provided within a table.

Chapter 4: Results

Research Question One

In this section, the following research question will be addressed, “What privacy and security risks exist within the top mHealth applications for headache disorders and what is their severity?” Table 10 provides a summary of the comparative risk analysis results of the top mHealth applications for headache disorders.

Table 10

Top mHealth Applications for HD Comparison Results

		Features												Total	Total (%)
		Create Account	Update Account Information	Data Storage	Export Data	GPS	Advertisements	* Delete Account	* Consumer Authentication	* Authenticate Each Use	* Password Policy	* Privacy Policy	* Compliance		
Applications	^s Acupressure: Heal Yourself (Android)	0	-	0	-	0	0	-	-	-	-	0	-	0	0
	Headache Log (Android)	0	-	1	1	0	1	-	1	-	-	0	1	5	63
	iMigraine (Android)	1	1	1	1	0	1	1	0	1	1	0	1	9	75
	^s Manage Your Pain Pro (Android)	1	1	1	1	0	0	1	0	1	1	0	1	8	67
	Migraine Buddy (Android)	1	1	1	1	1	0	1	0	1	1	0	1	9	75
	Migraine Diary (Android)	0	-	1	0	0	1	-	1	-	-	0	1	4	50
	Migraine eDiary (Android)	1	1	1	1	0	0	1	0	0	-	0	1	6	55

Migraine Relief Hypnosis (Android)	0	-	0	-	1	1	-	-	-	-	0	-	2	40
Relax Melodies (Android)	0	-	0	-	0	1	-	-	-	-	0	-	1	20
^s Acupressure: Heal Yourself (iOS)	0	-	0	-	0	0	-	-	-	-	0	-	0	0
^s Brainwave Tuner (iOS)	0	-	0	-	0	0	-	-	-	-	0	-	0	0
Curelator (iOS)	1	0	1	1	1	0	1	0	1	1	0	1	8	67
^s Headache Diary (iOS)	1	0	1	1	1	0	1	1	-	-	0	1	7	70
iHeadache (iOS)	0	-	1	1	0	0	-	1	-	-	0	1	4	50
iMigraine (iOS)	1	1	1	1	0	1	1	0	1	1	0	1	9	75
Migraine Buddy (iOS)	1	1	1	1	1	0	1	0	1	1	0	1	9	75
Migraine Coach (iOS)	1	1	1	1	1	0	1	1	-	-	0	1	8	80
Migraine eDiary (iOS)	1	1	1	1	0	0	1	0	0	-	0	1	6	55
Migraine Relief Hypnosis (iOS)	0	-	0	-	0	1	-	-	-	-	0	-	1	20
Relax Melodies (iOS)	0	-	0	-	1	1	-	-	-	-	0	-	2	40
Total	10	8	13	12	7	8	10	5	6	6	0	13		
Total (%)	50	80	65	92	35	40	100	38	75	100	0	100		

^s Paid Application * Poses Risk if Not Present

Privacy and Security Risks. Out of a total of 20 top mHealth applications for headache disorders, ten of the applications required the consumer to create an account and eight of the ten applications allowed the consumer to update their account information. All of the applications that required the consumer to create an account, required their first name, email address, gender, and age or date of birth to be entered. Four of the eight applications even required the consumer to enter their last name as well. However, one of the 10 mHealth applications for headache disorders,

Headache Diary for Android, that required the consumer to create an account, only required the consumer to enter a username instead of their first and last name. None of the top mHealth applications for headache disorders that required the consumer to create an account, allowed the consumer to delete their account when they no longer desired to use the application.

Sixty-five percent (or 13) of the 20 top mHealth applications for headache disorders, stored personal and medical data on the cloud or mobile device. Twelve out of the 13 mHealth applications for headache disorders that stored personal and medical data allowed the consumer to export their data to a document, email, cloud storage, or social media.

Eight of the 13 mHealth applications for headache disorders that stored personal and medical data required the consumer to authenticate. Of the eight mHealth applications for headache disorders that required the consumer to authenticate, only six applications allowed the consumer to create a password. The other two mHealth applications for headache disorders, Migraine eDiary for Android and iOS, required the consumer to create a four-digit personal identification number (PIN). All of the six mHealth applications for headache disorders that required the consumer to create a password, did not contain an adequate password policy. A majority of these applications only required the consumer to create an eight-character password and did not require the use of both uppercase and lowercase characters, numerical digits, or special characters. One of the six mHealth applications for headache disorders, Curelator for iOS, did require one numerical digit to be included in the eight-character password, however still did not meet the OWASP recommendations for implementing a strong password policy. Similarly, of the eight mHealth applications for headache disorders that required the consumer to authenticate, six did not require the consumer to authenticate each time they used the application. The other two mHealth applications for headache disorders, Headache eDiary for Android and iOS, that required

the consumer to authenticate using a four-digit PIN, did require the consumer to authenticate each time they used the application.

Forty percent (or eight) of the top mHealth applications for headache disorders contained advertisements. All of the mHealth applications for headache disorders that contained advertisements were free applications. Most of the advertisements were displayed at the bottom of the application, however two of the mHealth applications for headache disorders that contained advertisements, Migraine Relief Hypnosis for Android and iOS, were provided by the application developer within the application menu for specific medical-related products.

Thirty-five percent (or seven) of the 20 top mHealth applications for headache disorders allowed the use of GPS to determine the consumer's location in order to track weather conditions to assist in determining migraine triggers. However, two of the top mHealth applications for headache disorders, Migraine Buddy for Android and iOS, that did allow the use of GPS to determine the consumer's location, allowed the consumer to input a generalized location instead of, or in addition, to their exact location. For example, the consumer could state that the migraine episode occurred at home, work, etc. While this does not provide the ability to determine if certain weather conditions triggered a migraine episode, it allows the consumer to determine if other factors triggered the episode; such as: allergies to mold or dust, air quality, stress, etc.

All of the 20 top mHealth applications for headache disorders contained a privacy policy. The privacy policies varied in quality and thoroughness, but were accessible in both the appropriate application store and within the application itself.

None of the top 20 mHealth applications for headache disorders complied with any privacy and security guidelines or regulations.

Severity of the Privacy and Security Risks. Overall, the top mHealth applications for headache disorders had a medium severity. On average, the top mHealth applications for headache disorders contained 49 percent (or approximately six) of the 12 privacy and security risks. Fifteen percent (or three) of the top 20 mHealth applications for headache disorders contained none of the privacy and security risks. Seventy-five percent (or 15) of the top 20 mHealth applications for headache disorders contained at least three of the privacy and security risks. Sixty-five percent (or 13) of the top 20 mHealth applications for headache disorders contained at least six of the privacy and security risks. Twenty-five percent (or five) of the top 20 mHealth applications for headache disorders contained at least nine of the privacy and security risks. However, none of the top 20 mHealth applications for headache disorders contained all twelve of the privacy and security risks. Table 11 shows a summary of the total number of risks for the top 20 mHealth applications for headache disorders.

Table 11

Total Number of Risks for the Top mHealth Applications for HD

Applications with 0 Risks	3 of 20
Applications with 3+ Risks	15 of 20
Applications with 6+ Risks	13 of 20
Applications with 9+ Risks	5 of 20
Applications with All 12 Risks	0 of 20

According to the study, the top privacy and security risks for the top 20 mHealth applications for headache disorders are: compliance, password policy, delete account, export data, and update account information. None of the top 20 mHealth applications for headache disorders complied with any privacy and security guidelines or regulations, contained an adequate password policy, or allowed the consumer to delete their account. Ninety-two percent (or 12) of the applicable top 20 mHealth applications for headache disorders allowed the consumer to export their personal and medical data. Eighty percent (or eight) of the applicable top 20 mHealth

applications for headache disorders allowed the consumer to update their account information. Table 12 shows a summary of the top privacy and security risks for the top 20 mHealth applications for headache disorders.

Table 12

Top Risks for the Top mHealth Applications for HD

Compliance	100%
Password Policy	100%
Delete Account	100%
Export Data	92%
Update Account Information	80%

The study showed that the bottom privacy and security risks for the top 20 mHealth applications for headache disorders are: privacy policy, GPS, and consumer authentication. All of the top 20 mHealth applications for headache disorders contained a privacy policy. Only 35 percent (or seven) of the top 20 mHealth applications for headache disorders allowed the use of GPS. Only 38 percent (or five) of the applicable top 20 mHealth applications for headache disorders did not require the consumer to authenticate when accessing the application. Table 13 shows a summary of the bottom privacy and security risks for the top 20 mHealth applications for headache disorders.

Table 13

Bottom Risks for the Top mHealth Applications for HD

Privacy Policy	0%
GPS	35%
Consumer Authentication	38%

Research Question Two

In this section the following research question will be addressed, “Which mobile platform has the most severe privacy and security risks within their top mHealth applications for headache disorders?”

Android. Three studies were performed on the top Android mHealth applications for headache disorders. The first study consisted of all of the top Android mHealth applications for headache disorders, regardless of whether or not they were exclusive to the Android mobile platform. In order to provide a different perspective, the second study consisted of only those top Android mHealth applications for headache disorders that were not exclusive to the Android mobile platform and the third study consisted of only those top Android mHealth applications for headache disorders that were exclusive to the Android mobile platform.

Top Android mHealth Applications for Headache Disorders. Table 14 provides a summary of the comparative risk analysis results of the top Android mHealth applications for headache disorders.

Table 14

Top Android mHealth Applications for HD Comparison Results

		Features												Total	Total (%)
		Create Account	Update Account Information	Data Storage	Export Data	GPS	Advertisements	* Delete Account	* Consumer Authentication	* Authenticate Each Use	* Password Policy	* Privacy Policy	* Compliance		
Applications	^s Acupressure: Heal Yourself	0	-	0	-	0	0	-	-	-	-	0	-	0	0
	Headache Log	0	-	1	1	0	1	-	1	-	-	0	1	5	63
	iMigraine	1	1	1	1	0	1	1	0	1	1	0	1	9	75
	^s Manage Your Pain Pro	1	1	1	1	0	0	1	0	1	1	0	1	8	67
	Migraine Buddy	1	1	1	1	1	0	1	0	1	1	0	1	9	75

Migraine Diary	0	-	1	0	0	1	-	1	-	-	0	1	4	50
Migraine eDiary	1	1	1	1	0	0	1	0	0	-	0	1	6	55
Migraine Relief Hypnosis	0	-	0	-	1	1	-	-	-	-	0	-	2	40
Relax Melodies	0	-	0	-	0	1	-	-	-	-	0	-	1	20
Total	4	4	6	5	2	5	4	2	3	3	0	6		
Total (%)	44	100	67	83	22	56	100	33	75	100	0	100		

^s Paid Application * Poses Risk if Not Present

Overall, the top Android mHealth applications for headache disorders had a medium severity. On average, the top Android mHealth applications for headache disorders contained 49 percent (or approximately six) of the 12 privacy and security risks. Eleven percent (or one) of the top Android mHealth applications for headache disorders contained none of the privacy and security risks. Seventy-eight percent (or seven) of the top Android mHealth applications for headache disorders contained at least three of the privacy and security risks. Sixty-seven percent (or six) of the top Android mHealth applications for headache disorders contained at least six of the privacy and security risks. Twenty-two percent (or two) of the top Android mHealth applications for headache disorders contained at least nine of the privacy and security risks. None of the top Android mHealth applications for headache disorders contained all twelve of the privacy and security risks. Table 15 shows a summary of the total number of risks for the top Android mHealth applications for headache disorders.

Table 15

Total Number of Risks for the Top Android mHealth Applications for HD

Applications with 0 Risks	1 of 9
Applications with 3+ Risks	7 of 9
Applications with 6+ Risks	6 of 9
Applications with 9+ Risks	2 of 9
Applications with All 12 Risks	0 of 9

According to the study, the top privacy and security risks for the top Android mHealth applications for headache disorders are: compliance, password policy, delete account, export data, and update account information. None of the top Android mHealth applications for headache disorders complied with any privacy and security guidelines or regulations, contained an adequate password policy, allowed the consumer to delete their account, or allowed the consumer to update their account information. Eighty-three percent (or five) of the applicable top Android mHealth applications for headache disorders allowed the consumer to export their personal and medical data. Table 16 shows a summary of the top privacy and security risks for the top Android mHealth applications for headache disorders.

Table 16

Top Risks for the Top Android mHealth Applications for HD

Compliance	100%
Password Policy	100%
Delete Account	100%
Update Account Information	100%
Export Data	83%

The study showed that the bottom privacy and security risks for the top Android mHealth applications for headache disorders are: privacy policy, GPS, and consumer authentication. All of the top Android mHealth applications for headache disorders contained a privacy policy. Only 22 percent (or two) of the top Android mHealth applications for headache disorders allowed the use of GPS. Only 33 percent (or two) of the applicable top Android mHealth applications for headache disorders did not require the consumer to authenticate when accessing the application. Table 17 shows a summary of the bottom privacy and security risks for the top Android mHealth applications for headache disorders.

Table 17

Bottom Risks for the Top Android mHealth Applications for HD

Privacy Policy	0%
GPS	22%
Consumer Authentication	33%

Non-Exclusive Top Android mHealth Applications for Headache Disorders. Table 18 provides a summary of the comparative risk analysis results of the non-exclusive top Android mHealth applications for headache disorders.

Table 18

Non-Exclusive Top Android mHealth Applications for HD Comparison Results

		Features												Total	Total (%)
		Create Account	Update Account Information	Data Storage	Export Data	GPS	Advertisements	*Delete Account	* Consumer Authentication	* Authenticate Each Use	* Password Policy	* Privacy Policy	* Compliance		
Applications	^s Acupressure: Heal Yourself (Android)	0	-	0	-	0	0	-	-	-	-	0	-	0	0
	iMigraine (Android)	1	1	1	1	0	1	1	0	1	1	0	1	9	75
	Migraine Buddy (Android)	1	1	1	1	1	0	1	0	1	1	0	1	9	75
	Migraine eDiary (Android)	1	1	1	1	0	0	1	0	0	-	0	1	6	55
	Migraine Relief Hypnosis (Android)	0	-	0	-	1	1	-	-	-	-	0	-	2	40

Relax Melodies (Android)	0	-	0	-	0	1	-	-	-	-	0	-	1	20
Total	3	3	3	3	2	3	3	0	2	2	0	3		
Total (%)	50	100	50	100	33	50	100	0	67	100	0	100		

⁵ Paid Application * Poses Risk if Not Present

Overall, the non-exclusive top Android mHealth applications for headache disorders had a medium severity. On average, the non-exclusive top Android mHealth applications for headache disorders contained 44 percent (or approximately five) of the 12 privacy and security risks. Seventeen percent (or one) of the non-exclusive top Android mHealth applications for headache disorders contained none of the privacy and security risks. Sixty-seven percent (or four) of the non-exclusive top Android mHealth applications for headache disorders contained at least three of the privacy and security risks. Fifty percent (or three) of the non-exclusive top Android mHealth applications for headache disorders contained at least six of the privacy and security risks. Thirty-three percent (or two) of the non-exclusive top Android mHealth applications for headache disorders contained at least nine of the privacy and security risks. None of the non-exclusive top Android mHealth applications for headache disorders contained all twelve of the privacy and security risks. Table 19 shows a summary of the total number of risks for the non-exclusive top Android mHealth applications for headache disorders.

Table 19

Number of Risks for the Non-Exclusive Top Android mHealth Applications for HD

Applications with 0 Risks	1 of 6
Applications with 3+ Risks	4 of 6
Applications with 6+ Risks	3 of 6
Applications with 9+ Risks	2 of 6
Applications with All 12 Risks	0 of 6

According to the study, the top privacy and security risks for the non-exclusive top Android mHealth applications for headache disorders are: compliance, password policy, delete account,

export data, and update account information. None of the non-exclusive top Android mHealth applications for headache disorders complied with any privacy and security guidelines or regulations, contained an adequate password policy, allowed the consumer to delete their account, or allowed the consumer to update their account information. All of the non-exclusive top Android mHealth applications for headache disorders allowed the consumer to export their personal and medical data. Table 20 shows a summary of the top privacy and security risks for the non-exclusive top mHealth applications for headache disorders.

Table 20

Top Risks for the Non-Exclusive Top Android mHealth Applications for HD

Compliance	100%
Password Policy	100%
Delete Account	100%
Export Data	100%
Update Account Information	100%

The study showed that the bottom privacy and security risks for the non-exclusive top Android mHealth applications for headache disorders are: privacy policy, GPS, and consumer authentication. All of the non-exclusive top Android mHealth applications for headache disorders contained a privacy policy and required the consumer to authenticate. Only 33 percent (or two) of the non-exclusive top Android mHealth applications for headache disorders allowed the use of GPS. Table 21 shows a summary of the bottom privacy and security risks for the non-exclusive top Android mHealth applications for headache disorders.

Table 21

Bottom Risks for the Non-Exclusive Top Android mHealth Applications for HD

Privacy Policy	0%
Consumer Authentication	0%
GPS	33%

Exclusive Top Android mHealth Applications for Headache Disorders. Table 22 provides a summary of the comparative risk analysis results of the exclusive top Android mHealth applications for headache disorders.

Table 22

Exclusive Top Android mHealth Applications for HD Comparison Results

		Features												Total	Total (%)
		Create Account	Update Account Information	Data Storage	Export Data	GPS	Advertisements	* Delete Account	* Consumer Authentication	* Authenticate Each Use	* Password Policy	* Privacy Policy	* Compliance		
Applications	Headache Log	0	-	1	1	0	1	-	1	-	-	0	1	5	63
	^s Manage Your Pain Pro	1	1	1	1	0	0	1	0	1	1	0	1	8	67
	Migraine Diary	0	-	1	0	0	1	-	1	-	-	0	1	4	50
	Total	1	1	3	2	0	2	1	2	1	1	0	3		
	Total (%)	33	100	100	67	0	67	100	67	100	100	0	100		

^s Paid Application * Poses Risk if Not Present

Overall, the exclusive top Android mHealth applications for headache disorders had a high severity. On average, the exclusive top Android mHealth applications for headache disorders contained 60 percent (or seven) of the 12 privacy and security risks. Zero of the exclusive top Android mHealth applications for headache disorders contained none of the privacy and security risks. One-hundred percent (or three) of the exclusive top Android mHealth applications for headache disorders contained at least three of the privacy and security risks. One-hundred percent

(or three) of the exclusive top Android mHealth applications for headache disorders contained at least six of the privacy and security risks. None of the exclusive top Android mHealth applications for headache disorders contained at least nine of the privacy and security risks. None of the exclusive top Android mHealth applications for headache disorders contained all twelve of the privacy and security risks. Table 23 shows a summary of the total number of risks for the exclusive top Android mHealth applications for headache disorders.

Table 23

Number of Risks for the Exclusive Top Android mHealth Applications for HD

Applications with 0 Risks	0 of 3
Applications with 3+ Risks	3 of 3
Applications with 6+ Risks	3 of 3
Applications with 9+ Risks	0 of 3
Applications with All 12 Risks	0 of 3

According to the study, the top privacy and security risks for the exclusive top Android mHealth applications for headache disorders are: compliance, password policy, authenticate each use, data storage, update account information, and delete account. None of the exclusive top Android mHealth applications for headache disorders complied with any privacy and security guidelines or regulations, contained an adequate password policy, allowed the consumer to delete their account, allowed the consumer to update their account information, or required the consumer to authenticate each time they used the application. All of the exclusive top Android mHealth applications for headache disorders stored personal and medical data on the cloud or mobile device. Table 24 shows a summary of the top privacy and security risks for the exclusive top Android mHealth applications for headache disorders.

Table 24

Top Risks for the Exclusive Top Android mHealth Applications for HD

Compliance	100%
------------	------

Password Policy	100%
Authenticate Each Use	100%
Data Storage	100%
Update Account Information	100%
Delete Account	100%

The study showed that the bottom privacy and security risks for the exclusive top Android mHealth applications for headache disorders are: privacy policy, GPS, and create account. All of the exclusive top Android mHealth applications for headache disorders contained a privacy policy and did not allow the use GPS. Only 33 percent (or one) of the exclusive top Android mHealth applications for headache disorders required the consumer to create an account. Table 25 shows a summary of the bottom privacy and security risks for the exclusive top Android mHealth applications for headache disorders.

Table 25

Bottom Risks for the Exclusive Top Android mHealth Applications for HD

Privacy Policy	0%
GPS	0%
Create Account	33%

iOS. Similar to Android, three studies were performed on the top iOS mHealth applications for headache disorders. The first study consisted of all of the top iOS mHealth applications for headache disorders, regardless of whether or not they were exclusive to the iOS mobile platform. In order to provide a different perspective, the second study consisted of only those top iOS mHealth applications for headache disorders that were not exclusive to the iOS mobile platform and the third study consisted of only those top iOS mHealth applications for headache disorders that were exclusive to the iOS mobile platform.

Top iOS mHealth Applications for Headache Disorders. Table 26 provides a summary of the comparative risk analysis results of the top iOS mHealth applications for headache disorders.

Table 26

Top iOS mHealth Applications for HD Comparison Results

		Features												Total	Total (%)
		Create Account	Update Account Information	Data Storage	Export Data	GPS	Advertisements	*Delete Account	*Consumer Authentication	*Authenticate Each Use	*Password Policy	*Privacy Policy	*Compliance		
Applications	^s Acupressure: Heal Yourself	0	-	0	-	0	0	-	-	-	-	0	-	0	0
	^s Brainwave Tuner	0	-	0	-	0	0	-	-	-	-	0	-	0	0
	Curelator	1	0	1	1	1	0	1	0	1	1	0	1	8	67
	^s Headache Diary	1	0	1	1	1	0	1	1	-	-	0	1	7	70
	iHeadache	0	-	1	1	0	0	-	1	-	-	0	1	4	50
	iMigraine	1	1	1	1	0	1	1	0	1	1	0	1	9	75
	Migraine Buddy	1	1	1	1	1	0	1	0	1	1	0	1	9	75
	Migraine Coach	1	1	1	1	1	0	1	1	-	-	0	1	8	80
	Migraine eDiary	1	1	1	1	0	0	1	0	0	-	0	1	6	55
	Migraine Relief Hypnosis	0	-	0	-	0	1	-	-	-	-	0	-	1	20
	Relax Melodies	0	-	0	-	1	1	-	-	-	-	0	-	2	40
	Total	6	4	7	7	5	3	6	3	3	3	0	7		
	Total (%)	55	67	64	100	45	27	100	43	100	100	0	100		

^s Paid Application * Poses Risk if Not Present

Overall, the top iOS mHealth applications for headache disorders had a medium severity.

On average, the top iOS mHealth applications for headache disorders contained 48 percent (or

approximately six) of the 12 privacy and security risks. Seventeen percent (or two) of the top iOS mHealth applications for headache disorders contained none of the privacy and security risks. Sixty-seven percent (or eight) of the top iOS mHealth applications for headache disorders contained at least three of the privacy and security risks. Fifty-eight percent (or seven) of the top iOS mHealth applications for headache disorders contained at least six of the privacy and security risks. Twenty-five percent (or three) of the top iOS mHealth applications for headache disorders contained at least nine of the privacy and security risks. None of the top iOS mHealth applications for headache disorders contained all twelve of the privacy and security risks. Table 27 shows a summary of the total number of risks for the top iOS mHealth applications for headache disorders.

Table 27

Number of Risks for the Top iOS mHealth Applications for HD

Applications with 0 Risks	2 of 12
Applications with 3+ Risks	8 of 12
Applications with 6+ Risks	7 of 12
Applications with 9+ Risks	3 of 12
Applications with All 12 Risks	0 of 12

According to the study, the top privacy and security risks for the top iOS mHealth applications for headache disorders are: compliance, password policy, delete account, authenticate each use, and export data. None of the top iOS mHealth applications for headache disorders complied with any privacy and security guidelines or regulations, contained an adequate password policy, allowed the consumer to delete their account, or required the consumer to authenticate each time they used the application. All of the applicable top iOS mHealth applications for headache disorders allowed the consumer to export their personal and medical data. Table 28 shows a summary of the top privacy and security risks for the top iOS mHealth applications for headache disorders.

*Table 28**Top Risks for the Top iOS mHealth Applications for HD*

Compliance	100%
Password Policy	100%
Delete Account	100%
Authenticate Each Use	100%
Export Data	100%

The study showed that the bottom privacy and security risks for the top iOS mHealth applications for headache disorders are: privacy policy, advertisements, and consumer authentication. All of the top iOS mHealth applications for headache disorders contained a privacy policy. Only 27 percent (or three) of the top iOS mHealth applications for headache disorders contained advertisements. Only 43 percent (or three) of the applicable top iOS mHealth applications for headache disorders did not require the consumer to authenticate when accessing the application. Table 29 shows a summary of the bottom privacy and security risks for the top iOS mHealth applications for headache disorders.

*Table 29**Bottom Risks for the Top iOS mHealth Applications for HD*

Privacy Policy	0%
Advertisements	27%
Consumer Authentication	43%

Non-Exclusive Top iOS mHealth Applications for Headache Disorders. Table 30 provides a summary of the comparative risk analysis results of the non-exclusive top iOS mHealth applications for headache disorders.

Table 30

Non-Exclusive Top iOS mHealth Applications for HD Comparison Results

		Features													
		Create Account	Update Account Information	Data Storage	Export Data	GPS	Advertisements	* Delete Account	* Consumer Authentication	* Authenticate Each Use	* Password Policy	* Privacy Policy	* Compliance	Total	Total (%)
Applications	[§] Acupressure: Heal Yourself (iOS)	0	-	0	-	0	0	-	-	-	-	0	-	0	0
	iMigraine (iOS)	1	1	1	1	0	1	1	0	1	1	0	1	9	75
	Migraine Buddy (iOS)	1	1	1	1	1	0	1	0	1	1	0	1	9	75
	Migraine eDiary (iOS)	1	1	1	1	0	0	1	0	0	-	0	1	6	55
	Migraine Relief Hypnosis (iOS)	0	-	0	-	0	1	-	-	-	-	0	-	1	20
	Relax Melodies (iOS)	0	-	0	-	1	1	-	-	-	-	0	-	2	40
	Total	3	3	3	3	2	3	3	0	2	2	0	3		
	Total (%)	50	100	50	100	33	50	100	0	67	100	0	100		

[§] Paid Application * Poses Risk if Not Present

Overall, the non-exclusive top iOS mHealth applications for headache disorders had a medium severity. On average, the non-exclusive top iOS mHealth applications for headache disorders contained 44 percent (or five) of the 12 privacy and security risks. Seventeen percent (or one) of the non-exclusive top iOS mHealth applications for headache disorders contained none of the privacy and security risks. Sixty-seven percent (or four) of the non-exclusive top iOS mHealth

applications for headache disorders contained at least three of the privacy and security risks. Fifty percent (or three) of the non-exclusive top iOS mHealth applications for headache disorders contained at least six of the privacy and security risks. Thirty-three percent (or two) of the non-exclusive top iOS mHealth applications for headache disorders contained at least nine of the privacy and security risks. However, none of the non-exclusive top iOS mHealth applications for headache disorders contained all twelve of the privacy and security risks. Table 31 shows a summary of the total number of risks for the non-exclusive top iOS mHealth applications for headache disorders.

Table 31

Number of Risks for the Non-Exclusive Top iOS mHealth Applications for HD

Applications with 0 Risks	1 of 6
Applications with 3+ Risks	4 of 6
Applications with 6+ Risks	3 of 6
Applications with 9+ Risks	2 of 6
Applications with All 12 Risks	0 of 6

According to the study, the top privacy and security risks for the non-exclusive top iOS mHealth applications for headache disorders are: compliance, password policy, delete account, update account information, and export data. None of the non-exclusive top iOS mHealth applications for headache disorders complied with any privacy and security guidelines or regulations, contained an adequate password policy, or allowed the consumer to delete their account. All of the non-exclusive top iOS mHealth applications for headache disorders allowed the consumer to export their personal and medical data and update their account information. Table 32 shows a summary of the top privacy and security risks for the non-exclusive top iOS mHealth applications for headache disorders.

Table 32

Top Risks for the Non-Exclusive Top iOS mHealth Applications for HD

Compliance	100%
Password Policy	100%
Delete Account	100%
Export Data	100%
Update Account Information	100%

The study showed that the bottom privacy and security risks for the non-exclusive top iOS mHealth applications for headache disorders are: privacy policy, consumer authentication, and GPS. All of the non-exclusive top iOS mHealth applications for headache disorders contained a privacy policy and required the consumer to authenticate. Only 33 percent (or two) of the non-exclusive top iOS mHealth applications for headache disorders allowed the use of GPS. Table 33 shows a summary of the bottom privacy and security risks for the non-exclusive top iOS mHealth applications for headache disorders.

Table 33

Bottom Risks for the Non-Exclusive Top iOS mHealth Applications for HD

Privacy Policy	0%
Consumer Authentication	0%
GPS	33%

Exclusive Top iOS mHealth Applications for Headache Disorders. Table 34 provides a summary of the comparative risk analysis results of the exclusive top iOS mHealth applications for headache disorders.

Table 34

Exclusive Top iOS mHealth Applications for HD Comparison Results

		Feature												Total	Total (%)
		Create Account	Update Account Information	Data Storage	Export Data	GPS	Advertisements	* Delete Account	* Consumer Authentication	* Authenticate Each Use	* Password Policy	* Privacy Policy	* Compliance		
Application	^s Brainwave Tuner	0	-	0	-	0	0	-	-	-	-	0	-	0	0
	Curelator	1	0	1	1	1	0	1	0	1	1	0	1	8	67
	^s Headache Diary	1	0	1	1	1	0	1	1	-	-	0	1	7	70
	iHeadache	0	-	1	1	0	0	-	1	-	-	0	1	4	50
	Migraine Coach	1	1	1	1	1	0	1	1	-	-	0	1	8	80
	Total	3	1	4	4	3	0	3	3	1	1	0	4		
	Total (%)	60	33	80	100	60	0	100	75	100	100	0	100		

^s Paid Application * Poses Risk if Not Present

Overall, the exclusive top iOS mHealth applications for headache disorders had a high severity. On average, the exclusive top iOS mHealth applications for headache disorders contained 53 percent (or approximately six) of the 12 privacy and security risks. Twenty percent (or one) of the exclusive top iOS mHealth applications for headache disorders contained none of the privacy and security risks. Eighty percent (or four) of the exclusive top iOS mHealth applications for headache disorders contained at least three of the privacy and security risks. Eighty percent (or four) of the exclusive top iOS mHealth applications for headache disorders contained at least six of the privacy and security risks. Twenty percent (or one) of the exclusive top iOS mHealth applications for headache disorders contained at least nine of the privacy and security risks.

However, none of the exclusive top iOS mHealth applications for headache disorders contained all twelve of the privacy and security risks. Table 35 shows a summary of the total number of risks for the exclusive top iOS mHealth applications for headache disorders.

Table 35

Number of Risks for the Exclusive Top iOS mHealth Applications for HD

Applications with 0 Risks	1 of 5
Applications with 3+ Risks	4 of 5
Applications with 6+ Risks	4 of 5
Applications with 9+ Risks	1 of 5
Applications with All 12 Risks	0 of 5

According to the study, the top privacy and security risks for the exclusive top iOS mHealth applications for headache disorders are: compliance, password policy, authenticate each use, delete account, and export data. None of the exclusive top iOS mHealth applications for headache disorders complied with any privacy and security guidelines or regulations, contained an adequate password policy, required the consumer to authenticate each time they used the application, or allowed the consumer to delete their account. All of the exclusive top iOS mHealth applications for headache disorders allowed the consumer to export their personal and medical data. Table 36 shows a summary of the top privacy and security risks for the exclusive top iOS mHealth applications for headache disorders.

Table 36

Top Risks for the Exclusive Top iOS mHealth Applications for HD

Compliance	100%
Password Policy	100%
Authenticate Each Use	100%
Delete Account	100%
Export Data	100%

The study showed that the bottom privacy and security risks for the exclusive top iOS mHealth applications for headache disorders are: privacy policy, advertisements, and update

account information. All of the exclusive top iOS mHealth applications for headache disorders contained a privacy policy. None of the exclusive top iOS mHealth applications for headache disorders contained advertisements. Only 33 percent (or one) of the exclusive top iOS mHealth applications for headache disorders allowed the consumer to update their account information. Table 37 shows a summary of the bottom privacy and security risks for the exclusive top iOS mHealth applications for headache disorders.

Table 37

Bottom Risks for the Exclusive Top iOS mHealth Applications for HD

Privacy Policy	0%
Advertisements	0%
Update Account Information	33%

Summary. Each of the three studies for Android and iOS provides a different perspective of the results. The first study regarding the top Android and iOS mHealth applications for headache disorders as well as the second study regarding the non-exclusive top Android and iOS mHealth applications for headache disorders had a significantly less average severity than the third study regarding the mHealth applications for headache disorders exclusive to each mobile platform.

In two of the three studies, Android had a higher average severity than iOS. In one of the three studies, Android and iOS had an equal average severity. In the first and second studies, Android and iOS both had a medium average severity with an average of six of the 12 privacy and security risks. In the third study, Android and iOS both had a high average severity, but Android had an average of seven of the 12 privacy and security risks and iOS had six of the 12 privacy and security risks.

In the third study, which includes only the mHealth applications for headache disorders that were exclusive to each mobile platform, Android had a seven percent higher average severity and therefore had a higher number of average privacy and security risks as well. Overall, Android

had a higher average severity by three percent resulting in Android having a high average severity, while iOS had a medium average severity. Despite the severity difference, Android and iOS both contained an average of six privacy and security risks. Table 38 provides the average severities for both Android and iOS in each of the three studies, as well as an average of the three studies for each mobile platform.

Table 38

Average Severities of the Three Android and iOS Studies

	Mobile Platform Studies							
	Android				iOS			
	1	2	3	AVG	1	2	3	AVG
Average Severity	49%	44%	60%	51%	48%	44%	53%	48%

Note: Red = Higher, Yellow = Equal, Green = Lower

Research Question Three

In this section the following research question will be addressed, “What recommendations can be made to improve the privacy and security of personal and medical data within mHealth applications for headache disorders?” Table 39 provides a list of recommendations for improving the privacy and security of personal and medical data within mHealth applications for headache disorders for consumers and application developers. It is important to note that the recommendations provided, allows the features of the mHealth applications for headache disorders to still remain. It is not possible to eliminate all of the risks, even when eliminating these features from the mHealth applications for headache disorders. In addition, most of these features are critical to providing consumers with the ability to better manage their headache disorders. Therefore, these recommendations seek to provide a balance between the features of mHealth applications for headache disorders and security.

Table 39

Recommendations for Improving Privacy and Security of Personal and Medical Data

Consumers	Application Developers
Encrypt the mobile device to protect the stored data.	Review current government organization guidelines and regulations regarding the privacy and security of personal and medical data and implement if possible.
Use all of the privacy and security measures available on an application (i.e. application encryption, authentication, etc.).	Encrypt at-rest application data; including personal, medical, and location data.
Use a strong password for account and, if applicable, encryption of mobile device and/or the application.	Encrypt all in-motion data; including the personal and medical data that consumers export from the application.
Do not create an account unless required.	Alert the consumer or require verification when the consumer's account information is changed.
Only enter required personal and medical information when creating an account and using the application.	Do not include advertisements within the application; but if necessary ensure the legitimacy of the advertisement(s).
Delete the account when no longer desiring to use the application.	Create a password policy that follows the guidelines provided by OWASP.
Do not export personal and medical data unless necessary and verify destination.	If the consumer is allowed to create an account, allow the consumer to delete their account.
If the application does not require the consumer to authenticate each time they use the application, log out each time before closing the application.	If the consumer is allowed to create an account, require strong authentication each time the consumer uses the application.
Turn on and off GPS as needed; do not leave it on.	Do not share consumer's personal and medical data with third-parties.
Do not click on advertisements within the application.	Reduce the precision of the consumer's location to the city and state, instead of exact location.
Limit the amount of permissions the application uses and only grant permissions as necessary.	Create a thorough and descriptive privacy policy that tells the consumers how exactly their data will be used, who it will be shared with, and how it will be secured.
Do not allow the application to collect anonymous data.	
Research the application before using and also read the privacy policy first.	

Look for applications that comply with government organization guidelines and regulations.	
Rate the application within the application store and contact application developer with any concerns about the application.	

Chapter 5: Analysis and Suggestions for Further Study

Summary of Findings

Research Question 1. In this section, the following research question will be addressed, “What privacy and security risks exist within the top mHealth applications for headache disorders and what is their severity?” Overall, the top mHealth applications for headache disorders contained a medium average severity and 50 percent (or six) of the twelve privacy and security risks. The top mHealth applications for headache disorders contained all of the privacy and security risks except for privacy policy, because all of the applications contained a privacy policy. Compliance, password policy, delete account, export data, and update account information were the most prevalent privacy and security risks within the top mHealth applications for headache disorders. All of the applicable top mHealth applications for headache disorders did not comply with any guidelines or regulations, contain an adequate password policy, or allow the consumer to delete their account. Twelve of the 20 applicable top mHealth applications for headache disorders allowed the consumer to export their personal and medical data. Eight of the 20 applicable top mHealth applications for headache disorders allowed the consumer to update their account information. While GPS and consumer authentication were the least prevalent privacy and security risks within mHealth applications for headache disorders, they were still present in at least a third of the mHealth applications for headache disorders.

Research Question 2. In this section, the following research question will be addressed, “Which mobile platform has the most severe privacy and security risks within their top mHealth applications for headache disorders?” Android had a higher or equal average severity when compared to iOS in each of the three studies. In addition, Android had a three percent higher average severity among the three studies compared to iOS. The third study regarding the exclusive

mHealth applications for headache disorders for each mobile platform shows that those applications exclusive to Android contain more severe privacy and security risks. This is consistent with the results of each of the three studies that shows that Android has on average more privacy and security risks within their mHealth applications for headache disorders and their privacy and security risks are more severe than the iOS mHealth applications for headache disorders.

Research Question 3. In this section the following research question will be addressed, “What recommendations can be made to improve the privacy and security of personal and medical data within mHealth applications for headache disorders?” Table 39 provided the recommendations for improving the privacy and security of personal and medical data within mHealth applications for headache disorders. Application developers should first focus their attention on the top privacy and security risks within the top mHealth applications for headache disorders: compliance, password policy, delete account, export data, and update account information. Despite GPS and consumer authentication being the least prevalent privacy and security risks within the top mHealth applications for headache disorders, these should also be a focus for application developers as they are still present in over a third of the top mHealth applications for headache disorders. All of the top mHealth applications for headache disorders contained a privacy policy, however application developers should continue to implement privacy policies that are thorough in describing how consumers’ data will be used and protected.

Consumers should use caution and perform thorough research before downloading and using a mHealth application for headache disorders. Consumers should seek to download and use only those mHealth applications for headache disorders that comply with guidelines or regulations from government organizations. Consumers should limit the amount of personal and medical information they provide within the mHealth application for headache disorders by entering in

only required information. Consumers should turn off permissions and mobile device features, such as GPS, that are not being used within the mHealth application for headache disorders.

Comparison to Previous Studies

In a similar study performed by Adhikari, Richards, and Scott (2014), the privacy and security risks related to creating an account and storing personal and medical data on the cloud or mobile device were also determined to be prevalent risks within mHealth applications. Consumer authentication was determined by Adhikari et al. (2014) to not be a prevalent risk within mHealth applications, similar to this study. Adhikari et al. (2014) determined that deleting an account and update account information were not prevalent risks within mHealth applications. This study found that none of the mHealth applications for headache disorders allowed the consumer to delete their account and therefore ranked among the top privacy and security risks for mHealth applications for headache disorders. The study performed by Adhikari et al. (2014) determined that none of the mHealth applications within their study contained a privacy policy. However, this study found that all mHealth applications for headache disorders contained a privacy policy. It is important to note that the study performed by Adhikari et al. (2014) focused on the top mHealth applications and not specifically on headache disorder applications. The comparison to the Adhikari et al. (2014) study was of interest to the author as some of these privacy and security risks may have improved over the past four years or may be unique to headache disorder applications themselves.

Conclusion

mHealth applications for headache disorders pose a significant risk to the privacy and security of personal and medical data. Most mHealth applications for headache disorders contain half of the privacy and security risks that were included within this study. mHealth applications for headache disorders are not required to comply with HIPAA despite the fact that the medical

data used within these applications is just as sensitive as the data used by HIPAA-compliant entities. None of the mHealth applications for headache disorders complied with any government organization guidelines or regulations. Application developers are free to create mHealth applications for headache disorders as they desire and often seek to implement functionality and usability over privacy and security. Application developers need to implement privacy and security measures within their mHealth applications for headache disorders to protect personal and medical data and consumers need to make educated decisions when downloading and using these applications in order to better protect their personal and medical data.

Suggestions for Further Study

Due to the limitations of this study that provided a narrow focus on a specific sub-category of mHealth applications and specific features that pose as a risk to the privacy and security of personal and medical data, many different perspectives of the privacy and security risks were not covered in this study. The intention of this study was to focus on a specific sub-category of mHealth applications to provide a more accurate comparative risk analysis. It was also the intention of this study to focus on the most popular mHealth applications for headache disorders and the most common features within these applications that pose as a risk to the privacy and security of personal and medical data, in order to narrow the focus and provide recommendations that will benefit the most consumers.

During this study the author discovered other areas of interest that closely relate to the topics covered in this study, but were beyond the scope of this study. The following list includes suggestions for further study:

- Use different sub-categories of mHealth applications to determine the severity of headache disorder or general mHealth applications severity.

- Use different mHealth applications for headache disorder to confirm severity in mHealth applications for headache disorders.
- Use different features that pose as a risk to the privacy and security of personal and medical data, such as account verification.
- Use different mobile platforms to determine if privacy and security risks are as severe as they are on the Android mobile platform.
- Repeat the same study in the future to determine if the same privacy and security risks exist within the same mHealth applications for headache disorders and contain the same level of severity.

References

- Adhikari, R., Richards, D., & Scott, K. (2014). Security and privacy issues related to the use of mobile health apps. *ACIS*, 1-11. Retrieved January 18, 2018, from https://www.colleaga.org/sites/default/files/attachments/acis20140_submission_12.pdf
- Al-Zarouni, M. (2006). Mobile Handset Forensic Evidence: A Challenge for Law Enforcement. *Australian Digital Forensics Conference*, 1-11.
- Aspinall, D., & Knorr, K. (2015). Security Testing for Android mHealth Apps. *IEEE*, 1-8. Retrieved January 18, 2018, from <http://ieeexplore.ieee.org/abstract/document/7107459/>
- Axonoptics. (2017, February 21). *Top 5 Migraine Tracking Apps*. Retrieved February 1, 2018, from Axonoptics: <https://www.axonoptics.com/2017/02/top-5-migraine-tracking-apps/>
- Bacon, M., & Rouse, M. (2016, February). *Social Engineering*. Retrieved March 9, 2018, from TechTarget: <http://searchsecurity.techtarget.com/definition/social-engineering>
- Bacon, M., & Rouse, M. (2017, January). *Security*. Retrieved February 1, 2018, from TechTarget: <http://searchsecurity.techtarget.com/definition/security>
- Baum, S. (2015, November 15). *What separates the mobile health app “millionaires” from the rest?* Retrieved January 18, 2018, from MedCityNews: <https://medcitynews.com/2015/11/successful-mobile-health-app-developers/>
- Beal, V. (n.d.). *Mobile Operating System (OS)*. Retrieved February 1, 2018, from Webopedia: https://www.webopedia.com/TERM/M/mobile_operating_system.html
- Brewer, A. C., Buller, D. B., Dellavalle, R. P., Kamel-Boulos, M. N., & Karimkhani, C. (2014). Mobile Medical and Health Apps: State of the Art, Concerns, Regulatory Control and Certification. *Online Journal of Public Health Informatics*, 1-23. Retrieved January 18, 2018, from <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3959919/>

BusinessDictionary.com. (n.d.-a). *Android*. Retrieved February 1, 2018, from

BusinessDictionary.com: <http://www.businessdictionary.com/definition/Android.html>

BusinessDictionary.com. (n.d.-b). *iOS*. Retrieved February 1, 2018, from

BusinessDictionary.com: <http://www.businessdictionary.com/definition/iOS.html>

BusinessDictionary.com. (n.d.-c). *Social Media*. Retrieved March 9, 2018, from

BusinessDictionary.com: <http://www.businessdictionary.com/definition/social-media.html>

BusinessDictionary.com. (n.d.-d). *Unauthorized Access*. Retrieved March 9, 2018, from

BusinessDictionary.com: <http://www.businessdictionary.com/definition/unauthorized-access.html>

Cambridge Dictionary. (n.d.). *Guideline*. Retrieved March 9, 2018, from Cambridge Dictionary:

<https://dictionary.cambridge.org/us/dictionary/english/guideline>

Cole, B., & Margaret, R. (2016, November). *FTC (Federal Trade Commission)*. Retrieved February 1, 2018, from TechTarget:

<http://searchcompliance.techtarget.com/definition/FTC-Federal-Trade-Commission>

comScore, Inc. (2017, August 3). *comScore Reports June 2017 U.S. Smartphone Subscriber*

Market Share. Retrieved March 9, 2018, from comScore: <https://ir.comscore.com/news-releases/news-release-details/comscore-reports-june-2017-us-smartphone-subscriber-market-share>

Crawford, A., & Rouse, M. (2007, January). *Reverse Engineering*. Retrieved February 1, 2018, from TechTarget: <http://searchsoftwarequality.techtarget.com/definition/reverse-engineering>

engineering

- Dehling, T., Gao, F., Schneider, S., & Sunyaev, A. (2015). Exploring the Far Side of Mobile Health: Information Security and Privacy of Mobile Health Apps on iOS and Android. *JMIR mHealth and uHealth*, 3(1). doi:<http://doi.org/10.2196/mhealth.3672>
- Dehling, T., Mandl, K. D., Sunyaev, A., & Taylor, P. L. (2015). Availability and quality of mobile health app privacy policies. *Journal of the American Medical Informatics Association*, 28-33. doi:10.1136/amiajnl-2013-002605
- Dictionary.com. (n.d.). *Cyberattack*. Retrieved February 1, 2018, from Dictionary.com: <http://www.dictionary.com/browse/cyberattack>
- Driver, M. (2016, January 12). *Report Finds that 80% of 'Approved' mHealth Apps have at Least Two Major Security Flaws*. Retrieved January 18, 2018, from The Journal of mHealth: <http://www.thejournalofmhealth.com/single-post/2016/1/12/Report-Finds-That-80-of-%E2%80%98Approved%E2%80%99-mHealth-Apps-have-at-Least-Two-Major-Security-Flaws>
- Engel, K. (2018, March 12). *Have a Website? You Need a Privacy Policy. Here's Why*. Retrieved March 13, 2018, from Web Hosting Secret Revealed: <https://www.webhostingsecretrevealed.net/blog/blogging-tips/have-a-website-you-need-a-privacy-policy-heres-why/>
- Flaherty, J. L. (2014). Digital Diagnosis: Privacy and the Regulation of Mobile Phone Health Applications. *American Journal of Law & Medicine*, 40, 416-441.
- Fogg, C. (2014, October 21). *The 3 Types of mHealth Apps to Build Hospital Success*. Retrieved February 1, 2018, from MobileSmith: <https://www.nuemd.com/news/2017/06/05/5-apps-can-help-those-who-experience-migraines>

- Gunter, C. A., He, D., Nahrstedt, K., & Naveed, M. (2014). Security Concerns in Android mHealth Apps. *AMIA Annual Symposium Proceedings*, 645-654. Retrieved January 18, 2018, from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4419898/#__ffn__sectitle
- Harris, S. (2013). *CISSP All-in-One Exam Guide* (6th ed.). New York: McGraw-Hill Education.
- Heisler, Y. (2016, November 3). *Mobile Devices Become Most Popular Way to Access Internet*. Retrieved February 6, 2018, from New York Post: <https://nypost.com/2016/11/03/mobile-devices-become-most-popular-way-to-access-internet/>
- Hughes, A., Leake, A., & Rouse, M. (2017, February). *Database*. Retrieved March 27, 2017, from TechTarget: <https://searchsqlserver.techtarget.com/definition/database>
- Ireland, D. (2017, February 1). *An Underserved Market: Only 0.2% of Migraine Sufferers Use Migraine Apps*. Retrieved January 18, 2018, from Research 2 Guidance: <https://research2guidance.com/an-underserved-market-only-0-2-of-migraine-sufferers-use-migraine-apps-mobile-digital-health/>
- Johnson, D., Levinson, A., & Stackpole, B. (2011). Third Party Application Forensics on Apple Mobile Devices. *IEEE*, pp. 1-9.
- Kayl, R. A., Luxton, D. D., & Mishkind, M. C. (2012). mHealth Data Security: The Need for HIPAA Compliant Standardization. *Telemedicine and e-Health*, 18(4), 284-288. Retrieved January 18, 2018, from <http://online.liebertpub.com/doi/abs/10.1089/tmj.2011.0180>
- Kehoe, P. (2016, January 12). *2016 State of Application Security: Top Health Care Apps in Critical Condition*. Retrieved January 18, 2018, from Security Intelligence:

<https://securityintelligence.com/2016-state-of-application-security-top-health-care-apps-in-critical-condition/>

Landi, H. (2018, January 23). *2017 Breach Report: 477 Breaches, 5.6M Patient Records Affected*. Retrieved February 1, 2018, from Healthcare Informatics:

<https://www.healthcare-informatics.com/news-item/cybersecurity/2017-breach-report-477-breaches-56m-patient-records-affected>

Lord, N. (2016, June 13). *Data Protection: Data In transit vs. Data At Rest*. Retrieved March 27, 2018, from Digital Guardian: <https://digitalguardian.com/blog/data-protection-data-in-transit-vs-data-at-rest>

Martinez-Perez, B., & Torre-Diez, I. d. (2015). Privacy and Security in Mobile Health Apps: A Review and Recommendations. *Journal of Medical Systems*, 1-8. Retrieved January 18, 2018, from <https://link.springer.com/article/10.1007/s10916-014-0181-3>

McCarthy, K. (2017, June 5). *5 Apps That Can Help Those Who Experience Migraines*. Retrieved February 1, 2018, from NueMD: <https://www.nuemd.com/news/2017/06/05/5-apps-can-help-those-who-experience-migraines>

MCOL. (2015). *mHealth Fact Sheet*. Retrieved January 18, 2018, from mHealth Share: <http://www.mhealthshare.com/mfactsheet.htm>

MedicineNet.com. (n.d.). *HIPAA*. Retrieved February 1, 2018, from MedicineNet.com: <https://www.medicinenet.com/script/main/art.asp?articlekey=31785>

Merriam-Webster. (2018, January 16). *Migraine*. Retrieved February 1, 2018, from Merriam-Webster: <https://www.merriam-webster.com/dictionary/migraine>

Meyer, E. F. (2017, May 31). *Five Reasons Mobile Marketing is Becoming Even More Important*. Retrieved February 6, 2018, from Forbes:

<https://www.forbes.com/sites/forbesagencycouncil/2017/05/31/five-reasons-mobile-marketing-is-becoming-even-more-important/#cc97721abb48>

Migraine Research Foundation. (2017). *Migraine Facts*. Retrieved January 18, 2018, from Migraine Research Foundation: <http://migraineresearchfoundation.org/about-migraine/migraine-facts/>

Misra, S. (2014, November 20). *Majority of Android and iOS Apps Have Been Hacked, Including FDA-Cleared Health Apps*. Retrieved February 1, 2018, from iMedical Apps: <https://www.imedicalapps.com/2014/11/majority-top-android-ios-apps-hacked-including-fda-cleared-health-apps/>

National Institutes of Health. (2018, February 28). *mHealth*. Retrieved March 9, 2018, from National Institutes of Health: <http://searchhealthit.techtarget.com/definition/mHealth>

Oliveto, J. (2016, September 29). *The 6 Best Apps for Headaches and Migraines*. Retrieved February 1, 2017, from MigraineAgain: <https://migraineagain.com/apps-for-headaches-and-migraines/>

Open Web Application Security Project. (2017, April 27). *Top 10 Mobile Risks*. Retrieved February 1, 2018, from Open Web Application Security Project: https://www.owasp.org/index.php/OWASP_Mobile_Security_Project#tab=Top_10_Mobile_Risks

O'Reilly, K. B. (2017, September 20). *More Big Names Join Effort to Help Improve mHealth Apps*. Retrieved February 1, 2018, from AMA Wire: <https://wire.ama-assn.org/practice-management/more-big-names-join-effort-help-improve-mhealth-apps>

OWASP. (2017, April 21). *Authentication Cheat Sheet*. Retrieved March 3, 2018, from OWASP:

https://www.owasp.org/index.php/Authentication_Cheat_Sheet#Implement_Proper_Password_Strength_Controls

Oxford Dictionaries. (n.d.). *Black Market*. Retrieved February 1, 2018, from Oxford

Dictionaries: https://en.oxforddictionaries.com/definition/black_market

PC Magazine. (n.d.). *Application Developer*. Retrieved February 1, 2018, from PC Magazine:

<https://www.pcmag.com/encyclopedia/term/37897/application-developer>

Peleg, M., & Rouse, M. (2016, July). *Global Positioning System (GPS)*. Retrieved March 9,

2018, from TechTarget: <http://searchmobilecomputing.techtarget.com/definition/Global-Positioning-System>

Perrin, A., & Rainie, L. (2017, June 28). *10 Facts About Smartphones as the iPhone Turns 10*.

Retrieved January 24, 2018, from Pew Research: <http://www.pewresearch.org/fact-tank/2017/06/28/10-facts-about-smartphones/>

Pew Research Center. (2018, February 5). *Mobile Fact Sheet*. Retrieved February 7, 2018, from

Pew Research Center: <http://www.pewinternet.org/fact-sheet/mobile/>

Pohl, M. (2017). *325,000 Mobile Health Apps Available in 2017 - Android Now the Leading*

mHealth Platform. Retrieved January 18, 2018, from Research 2 Guidance:

<https://research2guidance.com/325000-mobile-health-apps-available-in-2017/>

Rouse, M. (2006, June). *OWASP Top Ten*. Retrieved February 1, 2018, from TechTarget:

<http://searchsoftwarequality.techtarget.com/definition/OWASP-Top-Ten>

Rouse, M. (2007, June). *Smartphone*. Retrieved February 1, 2018, from TechTarget:

<http://searchmobilecomputing.techtarget.com/definition/smartphone>

Rouse, M. (2011, November). *App*. Retrieved February 1, 2018, from TechTarget:

<http://searchmobilecomputing.techtarget.com/definition/app>

Rouse, M. (2012, April). *American Telemedicine Association (ATA)*. Retrieved February 1, 2018,

from TechTarget: <http://searchhealthit.techtarget.com/definition/American-Telemedicine-Association-ATA>

Rouse, M., & Steele, C. (2013, March). *App Store (Application Store)*. Retrieved February 1,

2018, from TechTarget: <http://searchmobilecomputing.techtarget.com/definition/app-store-application-store>

Rouse, M., & Sutner, S. (2016, September). *FDA (U.S. Food and Drug Administration)*.

Retrieved February 1, 2018, from TechTarget:

<http://searchhealthit.techtarget.com/definition/FDA-US-Food-and-Drug-Administration>

Rouse, M., & Vaughan, J. (2017, May). *Data*. Retrieved February 1, 2018, from TechTarget:

<http://searchdatamanagement.techtarget.com/definition/data>

Safeopedia. (n.d.). *Regulatory Compliance*. Retrieved March 9, 2018, from Safeopedia:

<https://www.safeopedia.com/definition/5431/regulatory-compliance>

Symantec. (2009, October 27). *Q&A for Newbies in Application Repackaging - Part 1*. Retrieved

February 1, 2018, from Symantec: <https://www.symantec.com/connect/blogs/q-newbies-application-repackaging-part-1>

Techopedia. (n.d.-a). *Mobile Device*. Retrieved February 1, 2018, from Techopedia:

<https://www.techopedia.com/definition/23586/mobile-device>

Techopedia. (n.d.-b). *Vulnerability*. Retrieved February 1, 2018, from Techopedia:

<https://www.techopedia.com/definition/13484/vulnerability>

Techopedia. (n.d.-c). *Authentication*. Retrieved March 9, 2018, from Techopedia:

<https://www.techopedia.com/definition/342/Authentication>

Techopedia. (n.d.-d). *Cloud Storage*. Retrieved March 9, 2018, from Techopedia:

<https://www.techopedia.com/definition/26535/cloud-storage>

Threat Analysis Group. (2010, May 3). *Threat, Vulnerability, Risk*. Retrieved February 1, 2018,

from Threat Analysis Group: <https://www.threatanalysis.com/2010/05/03/threat-vulnerability-risk-commonly-mixed-up-terms/>

Trend Micro. (n.d.). *Cybercriminals*. Retrieved February 1, 2018, from Trend Micro:

<https://www.trendmicro.com/vinfo/us/security/definition/cybercriminals>

U.S Department of Health and Human Services. (2013, January 24). *How Can You Protect and*

Secure Health Information When Using a Mobile Device. Retrieved February 1, 2018, from HealthIT.gov: <https://www.healthit.gov/providers-professionals/how-can-you-protect-and-secure-health-information-when-using-mobile-device>

Webopedia. (n.d.). *Feature*. Retrieved March 9, 2018, from Webopedia:

<https://www.webopedia.com/TERM/F/feature.html>

World Health Organization. (2016, April). *Headache Disorders*. Retrieved February 1, 2018,

from World Health Organization: <http://www.who.int/mediacentre/factsheets/fs277/en/>

Appendix A: OWASP Mobile Top 10 Risks¹

M1 - Improper Platform Usage	This category covers misuse of a platform feature or failure to use platform security controls. It might include Android intents, platform permissions, misuse of TouchID, the Keychain, or some other security control that is part of the mobile operating system. There are several ways that mobile apps can experience this risk.
M2 - Insecure Data Store	This new category is a combination of M2 + M4 from Mobile Top Ten 2014. This covers insecure data storage and unintended data leakage.
M3 - Insecure Communication	This covers poor handshaking, incorrect SSL versions, weak negotiation, cleartext communication of sensitive assets, etc.
M4 - Insecure Authentication	This category captures notions of authenticating the end user or bad session management. This can include: failing to identify the user at all when that should be required, failure to maintain the user's identity when it is required, and weaknesses in session management.
M5 - Insufficient Cryptography	The code applies cryptography to a sensitive information asset. However, the cryptography is insufficient in some way. Note that anything and everything related to TLS or SSL goes in M3. Also, if the app fails to use cryptography at all when it should, that probably belongs in M2. This category is for issues where cryptography was attempted, but it wasn't done correctly.
M6 - Insecure Authorization	This is a category to capture any failures in authorization (e.g., authorization decisions in the client side, forced browsing, etc.). It is distinct from authentication issues (e.g., device enrolment, user identification, etc.). If the app does not authenticate users at all in a situation where it should (e.g., granting anonymous access to some resource or service when authenticated and authorized access is required), then that is an authentication failure not an authorization failure.
M7 - Client Code Quality	This was the "Security Decisions Via Untrusted Inputs", one of our lesser-used categories. This would be the catch-all for code-level implementation problems in the mobile client. That's distinct from server-side coding mistakes. This would capture things like buffer overflows, format string vulnerabilities, and various other code-level mistakes where the solution is to rewrite some code that's running on the mobile device.
M8 - Code Tampering	This category covers binary patching, local resource modification, method hooking, method swizzling, and dynamic memory modification. Once the application is delivered to the mobile device, the code and data resources are resident there. An attacker can either directly modify the code, change the contents of memory dynamically, change or replace the system APIs that the application uses, or modify the application's data and resources. This can provide the attacker a direct method of subverting the intended use of the software for personal or monetary gain.
M9 - Reverse Engineering	This category includes analysis of the final core binary to determine its source code, libraries, algorithms, and other assets. Software such as IDA Pro, Hopper, otool, and other binary inspection tools give the attacker insight into the inner workings of the application. This may be used to exploit other nascent vulnerabilities in the application, as well as revealing information about back end servers, cryptographic constants and ciphers, and intellectual property.
M10 - Extraneous Functionality	Often, developers include hidden backdoor functionality or other internal development security controls that are not intended to be released into a production environment. For example, a developer may accidentally include a password as a comment in a hybrid app. Another example includes disabling of 2-factor authentication during testing.

¹ https://www.owasp.org/index.php/Mobile_Top_10_2016-Top_10