Mobile Health (mHealth): Modern Accessibility to Healthcare

Malaika Sheikh

IT-104-DL5

Professor Henderson

October 2, 2022

"By placing this statement on my webpage, I certify that I have read and understand the GMU Honor Code on https://oai.gmu.edu/mason-honor-code/ and as stated, I as student member of the George Mason University community pledge not to cheat, plagiarize, steal, or lie in matters related to academic work. In addition, I have received permission from the copyright holder for any copyrighted material that is displayed on my site. This includes quoting extensive amounts of text, any material 2 copied directly from a web page and graphics/pictures that are copyrighted. This project or subject material has not been used in another class by me or any other student. Finally, I certify that this site is not for commercial purposes, which is a violation of the George Mason Responsible Use of Computing (RUC) Policy posted on http://copyright.gmu.edu/?page_id=301 web site."

Introduction/Background

Mobile health, also known as mHealth, utilizes mobile technology in order to provide medical services to millions of people. The reason mHealth apps were created was to allow individuals to play a more significant role in their health by accessing healthcare services through something that millions of people use every day, which is technology. The rise of these mHealth apps began when the combination of handheld devices and cloud computer started to become more common among the population because then there could also be a way to access health-related apps 24/7. Some common mHealth apps include food-intake trackers, medication reminders, and fitness trackers. Current studies show that as of August 2022, 83% of the world's population owns a smartphone, with mHealth apps essentially becoming apps that are now commonly found as default apps (Petrovic, 2022). However, with the rise of mHealth applications, there are downsides to this development and those include security concerns that include medical information being leaked by hackers, and ethical concerns are also widespread because there is more medical information on the cloud now than ever before. Therefore, this research is important because it analyzes various aspects of mHealth apps in order to determine the best way to approach the advancement of health-related apps, while also considering a way to keep medical information confidential to the users themselves.

Current Use/Benefits

The wide variety of mHealth apps that are available on smartphones now means that there are various services that they provide. Some mobile health examples include Generis, which is an app that connects patients with diabetes to provide useful tips to each other, Apple Health, which monitors physical activity, heart rate, sleep, and food intake, and Headspace, which is a mental health app that allows users to explore guided meditation and audios for

relaxation (Bhatt, 2021). More recently, contact tracing apps became a hot topic in mHealth technology because of the rise of COVID-19, representing the significance of these apps in protecting the public. Not only that, but healthcare providers also make use of mHealth apps through virtual appointments, accessing images and scans, electronically prescribing medications, and scheduling appointments (Ventola, 2014, p. 358). This means that mHealth apps provide numerous services to patients and providers, which is why they are so beneficial to the public because it gives users an active role in taking care of themselves, and it also allows providers to be in contact with patients.

Security

With the convenience of being able to access healthcare services anytime, there does come a risk of security threats. That risk includes having medical and personal information being hacked. In a study conducted by Arxan, an American technology company that specializes in app-level security, they found that of 19 FDA approved mHealth apps that they analyzed for security, 84% of them did not address application code tampering and reverse engineering, which are 2 of the top ten security risks that apps face (Jolt, 2019). This means that since the mHealth apps are not addressing these significant security risks, they are much more vulnerable to having user medical information being hacked. This can be seen through the fact that global health data breaches had increased to 24.5% in 2020, and is rising, which means that there are various ways these mHealth apps are vulnerable to security threats. The reason for this is that since mobile health technologies transmit data through the atmosphere, this means that signals are vulnerable to active and passive attacks that can be intercepted, destroyed, hacked, and modified. It is found that the best way to protect mHealth apps from these risks is to implement two-factor authentication, lock access to the app after a number of incorrect login attempts, and

regularly update the apps to reduce vulnerability. However, there is another thing to worry about, which is security in terms of the Internet of Healthcare Things (IoHT). IoHT is the use of the Internet of Things in healthcare in which a network of cloud computing devices store medical information. For the IoHT, the best way to reduce security threats include adding blockchain technology, enabling encryption for health-related communication, and adding device verification. This displays how there are many ways that mHealth apps can tackle security risks that they are inevitably vulnerable to in order to keep the medical and personal health-related data of millions of users confidential. (Bajwa, 2022).

Legal and Ethical Issues

Security risks are not that only thing that mHealth apps need to worry about as there are also ethic and legal issues that come along with this because medical information is the type of information is very sensitive data. First of all, HIPAA (Health Insurance Portability and Accountability Act), is a US federal law that states that all healthcare providers need to maintain the confidentiality of all patient's medical information, which also includes mobile health apps. The thing is that since these mHealth apps are collecting medical information about an individual and storing that data onto the app, this means that these apps may have loopholes to share information with 3rd parties without making it clear to the users, which raises and ethical concern of not keeping medical information private. For example, Checkpoint Researchers, who are a part of a cyber threat intelligence company, conducted a study in which they analyzed the data of 23 apps on an android, and the number of downloads per app was between 10,000 and 10 million. The researchers found that app developers left the data of millions of users exposed to 3rd party cloud services by not following secure practices to integrate these 3rd parties, which included mHealth apps. This raised an ethical concern of having one's medical data being shared

with other companies in order to "improve" their performance (HT Tech, 2021). With this ethical concern, it raises a legal concern of the fact that users can sue these mHealth companies for sharing their medical information with 3rd parties without their knowledge or consent. This can lead to bigger consequences like legally having the mHealth apps shut down all together or having 3rd party companies investigated for their sharing of information. To make matters even more complicated, "there is no single federal agency or law that governs the vast realm of mHealth apps (Jolt, 2019)," which means that mHealth apps may be able to slip away with sharing medical information because they are not thoroughly regulated besides the general medical act, HIPAA, raising concern for if mHealth apps are even significantly part of the bigger conversation of "what should be done better to protect data of users."

Social Implications

Social implications of mHealth apps are also an important topic to discuss because since the general population has easy access to these apps, it does significantly impact the social aspect of healthcare. The fact is that more and more individuals are joining healthcare apps, which has been leading to an increase in health awareness and staying more fit in order to maintain the healthiest that one can be by keeping up with apps on one's phone. For example, one significant feature on mHealth apps is that users can communicate with each other, which introduces many people to new ideas and new methods of maintaining better health that one could not have accessed through a certain doctor. However, with this communication, people are also susceptible to being fed misinformation, which is very dangerous in terms of healthcare because it is important that people don't take steps that harm their physical well-being. This is why society needs to be careful about what information they follow on these mHealth apps by verifying recommendations and fact-checking what they see. Not only that, but another negative

social implication is that these apps can cause for paranoia as people may be coming overly obsessed or have an unhealthy obsession with physical and mental health apps. This is why mHealth apps should be used with caution, but also allow society to be more open to new medical services through equal consideration (Shor, 2021).

Future Use

The future of mHealth apps is diverse because they will not be gone anytime soon, in fact they are on the rise and expect to be among of the most widely used type of apps as the general population, healthcare providers, scientists, and researchers seek to increase the average lifespan and also further spread awareness about keeping up with one's health. Not only that, but people are starting to learn more about healthcare tips and tricks through mHealth apps, which has been contributing to society as a whole switching to new way of improving their physical and emotional well-being, and also helping researchers discover new scientific discoveries through the information that users willingly contribute to medical providers through these apps. It is also predicted that in the future, these mHealth apps will contribute to creating a more virtual healthcare system rather than face-to-face in situations not needed, connecting mHealth apps with physical devices, and contributing to the need for more research being done in terms of medical research. Through this, more and more people will want to utilize these apps in order to be educated, and therefore take better care of themselves. (Kelli et al., 2017, 206-208).

Conclusion

As can be analyzed, mHealth apps are used among millions of people across the world in order to monitor their health and are also used by healthcare providers to connect with their patients and access medical records. With the fact that people can access mHealth apps through the touch of a finger, this also means that security needs to be much tighter because sensitive

data cannot afford to be leaked to hackers. Furthermore, these mobile health apps face ethical and legal challenges because again, this private information does get shared with unauthorized 3rd parties but are challenging to fight against because there is no law that specifically governs healthcare apps. With the security, ethical, and legal concerns, there does come a bright side that society is coming together to improve their health altogether and be active in maintaining physical and mental well-being. Overall, mHealth will be staying with us in the long term, which is why we need to find the most optimal way to utilize these apps while securely taking care of sensitive information.

References

Bajwa, M. (2022, July 19). *Mobile Health (mHealth) security matters and mitigation*. Journal of AHIMA. Retrieved October 2, 2022, from https://journal.ahima.org/page/mobile-health-mhealth-security-matters-and-mitigation-10

- The journal above talks about how security relates to mobile health. The topics covered included physical, network, application, and user security, which are all a part of protecting the data of users utilizing mHealth applications. Furthermore, the journal provides solutions to increasing security of these apps so that sensitive information is protected and is not as vulnerable to cyberthreats anymore. As the journal goes on to explain mHealth security, it displays its credibility through detailed information that describes how and why mHealth apps are vulnerable to security threats. Credibility is also determined through the fact that the author has a PhD, which displays that the author is knowledgeable in the content.

Bhatt, S. (2022, September 9). *Top 12 most popular healthcare applications examples*. BoTree Technologies. Retrieved October 2, 2022, from https://www.botreetechnologies.com/blog/most-popular-healthcare-applications-examples/

- The article above lists examples of the 12 most popular health applications that are used today. Within the list, the author explains the purpose of each app and how it is utilized by healthcare providers and patients. One more thing to note about the article is that it explains how to work through the app, which gives the reader and idea of how mHealth apps are designed. The reason this source was cited in the research paper is because it gives significant example of mHealth apps that can be conveyed

throughout the research in order to give examples of what the paper is talking about. Furthermore, the article is credible because the author, Shardul Bhatt, states that he has been in the technical industry since 2002 and has been building the BoTree Technologies Company since 2012, which displays that he has long-term experience in this topic.

Compliancy Group. (2022, May 6). *Risks of mobile health apps: Are health apps putting phi at risk?* Compliancy Group. Retrieved October 2, 2022, from https://compliancy-group.com/risks-of-mobile-health-apps-security/

- The website above explains how mobile health apps are putting protected health information at risk because of the fact that that data is stored in a cloud-based service that hackers can easily access. The website then goes onto provide evidence through a study that was conducted about mHealth security and explains the significant findings of the study. The website was utilized in the paper in order to provide background information of why mHealth apps are at risk of security threats and why that is such a thing. One thing to note about the website is that it does contain an interview from David Stewart who is the CEO of the Approov Mobile Protection App, which adds credibility to the information that is being provided. This is because since he is the CEO and founder, it displays that he has experience and is knowledgeable of tech-security.

HT Tech. (2021, May 20). *Personal data of over 100 million Android users exposed by mobile app developers: Report*. HT Tech. Retrieved October 2, 2022, from https://tech.hindustantimes.com/tech/news/personal-data-of-over-100-million-android-users-exposed-by-mobile-app-developers-report-71621517149870.html

- This article focused on one specific study that was conducted which resulted in the findings that over 100 million Android users had their personal information exposed to 3rd parties. This article was incorporated in the research paper by utilizing the study as an example of how mHealth apps do have ethical and legal issues that need to be addressed. Furthermore, the source above highlighted how the medical data of millions of people across the world is being leaked to 3rd parties, which emphasizes the problem at hand. Furthermore, this research is reliable because it was conducted by the Checkpoint Tech Company, which is a tech company specialized in this aspect of technology. Also, the research does provide statistics, which also add credibility to the article by giving hard evidence to back up their reasoning.

Jolt. (2019, March 9). *Mobile health apps and legal uncertainty*. Richmond Journal of Law and Technology. Retrieved October 2, 2022, from https://jolt.richmond.edu/2016/11/07/mobile-health-apps-and-legal-uncertainty/

- The article above focuses on the legal aspect of mHealth apps. More specifically, this article talks about governing regulations, privacy, and security issues regarding the release of medical information of users utilizing these apps. The article engages in a conversation with other sources by adding their information into the source above in order to provide a plethora of information. Also, this source is reliable because at the end of the article, the author cites all the sources that was utilized to conduct the research. Also, there are numerous sources cited that display that through research was done before publishing this article.

Kelli, H. M., Witbrodt, B., & Shah, A. (2017, January 10). *The future of mobile health applications and devices in Cardiovascular Health*. European medical journal.

Innovations. Retrieved October 2, 2022, from https://pubmed.ncbi.nlm.nih.gov/28191545/

- The journal above goes into depth about what the future of mobile health will look like and how that specifically relates to devices in cardiovascular health because of the rapid advancement of these applications. Furthermore, the journal gives and overview of why mobile health is becoming much more popular. In the research paper, this journal was similarly used to describe the "future use" of mHealth applications because that is the category that it best fit in. Furthermore, the information provided is deemed reliable because this journal was constructed by individuals that are part of a medical university. That medical university is the Emory University School of Medicine, which displays that the authors are practicing in the field and are knowledgeable.

Petrovic, V. (2022, September 2). *What is mobile health and how it fits into Digital Health*. Vicert. Retrieved October 2, 2022, from https://vicert.com/what-is-mobile-health-and-how-does-it-fit-into-digital-health/

- This blog focuses on providing background information on what exactly mobile health is. For example, the article talks about the market for mHealth, the benefits of mHealth, and the challenges that come with these apps. The reason this article was used in the research was because it was the foundation to understanding what mobile health applications provide to users. Reliability in this blog is established by incorporating graphs that display the mHealth market, showing that there is evidence to back the author up. Furthermore, the author touches base with general mHealth

terms that are commonly accepted, which shows that he author knows what they are talking about.

Shor, R. (2021, May 5). *How health apps are changing social determinants of health*. PharmiWeb.com. Retrieved October 2, 2022, from https://www.pharmiweb.com/article/how-health-apps-are-changing-social-determinants-of-health

- The article above talks about how mobile health applications impact society. The article focuses on sub-topics like patient awareness, digital determinants of health, and the future of how mHealth apps will impact society. The article breaks this information down so that the reader gets and understanding of how greatly society is impacted by mobile health applications and that the impact will be greater in the future. This emphasis indicates that more research should be done to see what exactly the world should expect in the near future. Furthermore, this article was utilized in this research by adding it into the social implications section because that is what was best fit for the research and relevant.

Ventola, C. L. (2014, May). *Mobile devices and apps for Health Care Professionals: Uses and benefits*. P & T : a peer-reviewed journal for formulary management. Retrieved October 2, 2022, from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4029126/

- The article above goes into general information about how mobile health applications are used and what the benefits are. The article is broken down into similar sections like introduction, prevalence, the need of mHealth, and maintenance. The breaking down of information into these sub-sections makes the information easier to understand and realize what the author is actually talking about. This article was

incorporated into this research by adding it into the “current use/benefits” section because that is what the article provided more information of among all the sub-sections. Furthermore, the information is reliable in the article because the author, C. Lee Ventola, is a consultant medical writer, which displays that she is knowledgeable in this area.