Universiteit Leiden
ICT in Business

mHealth Applications:
Keeping Personal Electronic Health Records on Mobile Devices Confidential and Secure

Name: Andrews Himah

Date: July 2017

1st supervisor: Mr. Tino de Rijk
2nd supervisor: Dr. Arno Knobbe

MASTER'S THESIS

Leiden Institute of Advanced Computer Science (LIACS)
Leiden University
Niels Bohrweg 1
2333 CA Leiden
The Netherlands

MASTER'S THESIS

mHealth Applications: Keeping Personal Electronic Health Records on Mobile Devices Confidential and Secure

Andrews B. Himah
andrewsbhimah@gmail.com

In partial fulfilment of the requirements for the degree of

Master of Science (M.Sc.) of ICT in Business

Graduation: July 2017

Supervisor: Mr. Tino de Rijk

Second reader: Dr. Arno Knobbe

Leiden Institute of Advanced Computer Science (LIACS)

Leiden University

Niels Bohrweg 1

2333 CA Leiden

The Netherlands

Acknowledgements

There are numerous people, too many to list here, who have assisted me throughout the years with my academic work and especially with this thesis. I am grateful to everyone who helped me, but I owe a special debt of gratitude to my first supervisor, Tino de Rijk (Mr.) and second reader Arno Knobbe (Dr.), for their support and their comments, which contributed to my thesis and gave me the motivation and energy to complete this endeavour.

I would also like to thank all my friends and family who stood by me throughout this process and who, through their love and support, enabled me to fulfil this task.

Abstract

The principal aim of this study is to identify the potential threats that exist in terms of collecting and storing data on mobile phones and to suggest effective solutions for handling such personal electronic health data. As the world of technology is evolving, so is the healthcare industry and its use of mobile devices to manage personal medical data. This is a positive development, but the expansion of the use of mobile devices in the health industry also carries with it inherent dangers and potential problems that need to be investigated and addressed. This was the goal of the research reported on in this study.

Initially, the health industry made extensive use of paper records; however, the digital age introduced the use of computer systems to handle patients' medical records, which eventually led to the use of mobile technology to collect and store health-related information (mHealth). However, this evolution requires a critical assessment of the vulnerabilities in relation to personal medical information. The research carried out by this study has combined literature reviews, interviews, and surveys in order to reach the conclusions found in this critical assessment. The findings clearly show that the privacy and security of personal electronic health data on mobile devices cannot be guaranteed because of the lack of regulations in regard to confidentiality and security in relation to the mHealth market. Adequate security and confidentiality measures are still not in place and the crucial actors involved need to create the appropriate mechanisms that will help to mitigate the risks involved. All of this has meant that outside parties can gain access to patients' personal information without permission. In light of these findings, the recommendation has been made to institute a certification process that will test if all the required security mechanisms have been put into place, thus ensuring that granular control over user's data can be guaranteed.

Table of Contents

1 Introduction

1.1 Introduction

The digital world and the healthcare industry are constantly evolving. For example, nowadays, it is difficult to imagine living without a smartphone. Electronic health, or 'eHealth', was established a few years ago and is providing a catalyst for the development towards a fully-fledged *'mHealth'* (or mobile health) industry, which creates, accesses, and stores medical data through mobile devices such as smartphones and tablets.

This paper researches trends in the number of patients having access to electronic health records on their personal mobile devices or being able to create their own personal electronic health records using 'apps' on their mobile devices. Mobile apps are being developed and are already available that claim to be able to monitor health by taking readings with respect to certain physical or chemical measurements, thus reducing the need for regular visits to a local general practitioner (GP). The focus of this research paper is an analysis of how secure the personal sensitive data is that is being produced and accessed using so-called mHealth apps on patients' personal devices.

This trend of mHealth is, unfortunately, not being accompanied by a concomitant development in guidelines, legal frameworks, and procedures to ensure that the data being created, stored, and shared using these devices and software are safe and free from intrusion. It is well known that there are third parties for whom personal data, no matter how insignificant that information is to the user, is worth a lot of money. Third parties can use personal sensitive data for other means, against the will of the patient. Such data may include health records that health insurers or employers can use when considering contractual terms or targeted 'phishing' scams that are specific about a person's medical condition. What important is that the privacy and security of personally sensitive data accessed and stored on your mobile device can be guaranteed. The European Data Protection Law describes personal data as the following:

> **'Personal data'** means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person (European Parliament and Council of European Union, 2016).

Whether eHealth apps are, indeed, suitable substitutes for regular visits to a healthcare professional or whether the medical professional can access enough vital information through electronic health

records (EHR) about your medical condition by means of a mobile device is beyond the scope of this research.

1.2 Research motivation

We are seeing a prolonged, rapid growth in the smartphone industry. It is likely that in a couple of years society will accept the phenomenon of mHealth applications. In light of this, it is of great importance that sensitive personal health information that is created on mobile devices is secure and protected. Similarly to commercial aviation, which is also not 100% safe, security concerns are a booming industry that will require continuous assessment and improvement of security measures and procedures so that the ideal of 100% security and confidentiality can be attained. As more patients and health-oriented consumers are accessing and storing more personal sensitive health data on their mobile devices, the threat to this personal data is increasing. Research into these threats and how to minimise them are critically important as the acquisition of this kind of data grows in popularity and complexity. As the trend to store this kind of data grows, so do the number of third parties that wish to access this personal data either for purposes that might not always be clear or revealed to the patient (user). For example, if someone applies for a job and the interviewer has access to health information that states that the interviewee might not be in the best of health, that person's application might be rejected. Thus any such misuse of personal sensitive information on mobile devices needs to be prevented.

In a recent paper released by the IBM, that company stated that health industries were the biggest target of cyber-security attacks in 2015, a point in time known as 'the year of the healthcare breach'. IBM also provided a statement on why healthcare data is particularly interesting to hackers:

> "[Health records] typically contain credit card data, email addresses, social security numbers, employment information and medical history records – much of which will remain valid for years, if not decades. Cyber-thieves are using that data to launch spear-phishing attacks, commit fraud and steal medical identities" (IBM, 2016).

Patient-doctor confidentiality, personal data, and sensitive information may all be threatened by current trends. It is therefore important to secure medical records being stored on mobile devices.

The results of this research should benefit the three principal parties involved: the patients, the app providers, and the healthcare professionals because:

- Patients (users) will be able to understand what steps are needed to make their medical records safe when accessing their own private medical data.

- App providers (developers) will know more about what patients' desires and (more importantly) security concerns are and therefore will direct capital to the appropriate research and development that will reduce threats or at least warn consumers of the associated risks. A scandalous leakage of personal data could severely damage a company's reputation as it is developing such apps and could also undermine its competitive advantage in the marketplace.
- Health professionals will also understand the potential threats and can anticipate ways to detect and prevent them, whilst also having the confidence to inform patients about using approved and regulated mHealth applications. Concerns about confidentiality also play a crucial role here.

The purpose of this research is to recommend and enhance the security of personal electronic health records that are stored and accessed through mobile devices; hopefully, the findings will contribute to a safer and more secure environment for handling personal sensitive information. Furthermore, the public/users will be aware of the threats in mHealth apps and all the parties involved can contribute to mitigating the chance of attacks on this sensitive health data. More detail about all of these observations will be provided in Chapter 5. Other parties, like app developers, will need to understand and observe the appropriate regulations that have been drafted to ensure a secure environment. The gap between the effectiveness of healthcare industry and potential exposure of personal sensitive information needs to be filled.

1.3 Research statement

The research was undertaken in regard as to how to enhance the privacy and security of personal sensitive information on mobile devices focused on investigating and understanding the following issue:

> Potential threats to personal electronic health records (EHR), especially those data that are cloud-based or stored locally and thus accessible on mobile devices, need to be identified so that steps can be taken to protect client confidentiality.

The research carried out was based on the above thesis statement and relevant questions and objectives were investigated and clarified. The principal aim was to identify potential threats and to suggest effective solutions for handling personal EHR data on mobile devices.

Some additional objectives included:

- defining the benefits and threats to patients having independent access to their EHR data on their mobile devices;
- analysing the security of the current application programming interfaces (APIs) and apps available in the market for handling EHR data on mobile devices;
- identifying technologies that might contribute to a more secure usage of data on mobile devices; and
- specifying what is additionally needed on top of the default security measures in mobile devices when they contain and handle EHR data.

The principal research question was, therefore:

What can be done to enhance the security and confidentiality of personal EHR data stored and handled on mobile devices whilst granting patients more granular control over their data?

Additional questions included:

(1) What are the benefits and threats of using EHR on mobile devices?
(2) How secure are the current available apps and APIs (application programming interfaces) on the market that handle EHR data on mobile devices?
(3) Are there existing technologies that can improve data security and the storage on mobile devices?
(4) What specific additional mechanisms are needed on top of default security measures in mobile devices that contain and handle EHR data to improve medical confidentiality?

1.4 Research approach

An exploratory study has been utilised to conduct this research, an approach that combines qualitative research related to interviews and quantitative research related to surveys. A literature review has also taken place in order that more insight can be gained about the topic and the current status of the privacy and security of mHealth applications.

Table 1 outlines the approaches taken to answer the research questions.

Table 1: Research questions and approach

Research question	Research approach
1: What are the benefits and threats of using EHR on mobile devices?	Literature review Interviews

	Surveys
2: How secure are the current available APIs (application programming interfaces) and applications on the market that handle EHR data on mobile devices (Apple IOS and Google Android)?	Literature review Analysis on the literature Interviews Surveys
3: Are there existing technologies that can improve data security on mobile devices and where the data is stored?	Literature review Interviews
4: What specific additional mechanisms are needed on top of default security measures in mobile devices that contain and handle EHR data to improve medical confidentiality?	Literature review Interviews
Main question: What can be done to enhance the security and confidentiality of Personal EHR data stored and handled on mobile devices whilst granting patients more granular control over their data?	Based on approaches applied in the other research questions

1.5 Thesis outline

After Chapter 1 (the Introduction), the thesis contains the following:

- Chapter 2 starts with a background of eHealth and security and illustrates the origins and evolution of eHealth towards mHealth in order to highlight the crucial importance of security in the development of this new trend.
- Chapter 3 describes the methods used. This chapter gives a deeper insight into the methods and techniques applied in this research.
- Chapter 4 presents the results of the research carried out by means of the methods used in this research. This chapter contains the literature review and the results from the interviews and surveys.
- Chapter 5 presents the discussion, analysis, and findings on mHealth in regard to the risks and measures to be applied to ensure security and confidentiality.
- Finally, Chapter 6 discusses the conclusions of the research and answers all the questions that were originally posed. In addition, recommendations for future research are also given.

2 eHealth and security

2.1 Background of eHealth

Towards the end of the 20th century and up until this moment in time, a considerable number of industries and institutions have abandoned working solely with pen and paper and initially adopted rudimentary computer systems, which then became increasingly advanced in terms of sophistication, networking capabilities, and processing power. For example, the medical industry has made enormous strides and makes use of devices that can determine an illness, monitor a patient's health, assist patient recovery, and share information instantly within and between institutions (Cousin, Castilo-Hi, Snyder, 2015). These technological innovations have revolutionised patient care. The techniques through which data is stored on a mass scale and how it can be connected to other computers and servers has also witnessed a radical transformation.

'Electronic health', a term used during the initial stages of these developments, has evolved into the more recent term, 'eHealth', and involves healthcare practices being carried out through digital processes and communication hardware, all supported by customised software. With the rise of personal devices such as tablets and smartphones, the potential for doctors and patients to make use of mobile health-related software and harness device peripherals has not gone unnoticed. Defining the term 'eHealth' appropriately, however, has been an ongoing academic pursuit. The analysis contained here makes use of the most recent and accredited definitions available in relation to any ambiguous but important terms. The World Health Organisation (WHO) describes eHealth as the use of information and communication technologies (ICT) for health-related medical purposes (WHO, 2015).

The proliferation of health-related apps stored on mobile devices meant that, suddenly, personal health data was being stored on an increasing number of local and remote storage facilities. Many observers say that the scramble amongst app developers to fill the gap in the eHealth app market was a more pressing concern than the security of the private data being shared with others or kept on cloud-based storage. This means that the ways in which unwanted third-parties are able to access and replicate data sources are becoming ever more sophisticated and, following many security breaches of both individuals and institutions worldwide, consumers and health-care professionals are now having to reconsider their relationship with this new technology. In other words, the technology developed faster than the means of supervising and controlling it (Martinez-Perez, del Torre-Diez, Lopez-Coronado, 2015).

2.2 Security

Security is a crucial issue in the transport and storage of personal sensitive information on mobile devices. There are a number of stakeholders that have an interest in ensuring the confidentiality of information and they have the ability to influence the effectiveness of the privacy and security of personal EHR stored on mobile devices. Preliminary research indicated that the following groups were interested in these issues. They were:

- Application developers: This group understands that, if they do not take the appropriate measures to ensure proper data security, vulnerabilities might emerge, a development that would open the door for hackers to access and exploit the data.
- The users: If this group shares the passwords of their devices with others, an unauthorised user can subsequently get access to the phone and the information it contains. A recent study reported that about 41% of those who use smartphones in the health sector have no password protection on their phones. Furthermore, more than half of the users surveyed admitted that they have used unknown, sometimes unprotected, networks with their devices. Another scenario involves the user emailing personal health information to a wrong recipient rather than to the correct one, leading to the revealing of personal health information to unauthorised recipients. Human error and lack of vigilance are exploited by malicious information collectors (Zubaydi, Saleh, Aloul, & Sagahyroon, 2016).

These two actors have direct control of the security of personal health data on mobile devices. Chapter 5.1 delves deeper in terms of identifying the actors that share risks and makes suggestions as to how these risks can be mitigated in order to create a secure environment for storage of personal EHR on mobile devices.

2.2.1 Definition of security

The 2017 edition of the HIMSS Dictionary of Health Information
Technology Terms, Acronyms, and Organisations (p.102) defines health information security as ‘the reference to physical, technological, or administrative safeguards or tools used to protect identifiable health data from unwarranted access or disclosure’.

According to the Health Insurance Portability and Accountability Act (HIPAA, explained later on in this paper), the physical, technological, and administrative safeguards associated with the standard definition of ‘security’ from the data security point of view are:

Physical safeguards, which include making certain areas of storage facilities restricted areas that are not accessible to unauthorised visitors or certain personnel. These measures also include the regulation of workstations and other media usage and policies and routines that cover the transfer, deletion, disposal, and recycling of electronic media storage devices to ensure appropriate protection of electronic protected health information (also known as ePHI). A physical safeguard might also involve a void in the network that requires a physical interaction, such as confirmation by an authorised human user, that certain information can pass through to its desired destination, such as an 'airgap' in networking (U.S. Department of Health and Human Services, 2013).

Technological safeguards (known as technical safeguards in HIPAA) implies implementing hardware-, software and/or process measures that record, track, and monitor instances of access and use of data. Much like the physical safeguards, technological safeguards have a lot to do with access-level controls to personal health data and how they are maintained by the system. For example, users can be granted different levels of reading and editing rights by an active directory. Electronic mechanisms are employed that prevent the unwarranted or accidental deletion or adjustment of personal health data (HIMSS, 2017). Technological safeguards, such as firewalls and malware scanners, are also put in place and detect and prevent intrusion and infection. These are able to run 24 hours a day and search for unwanted intruder software and remote infiltration (U.S. Department of Health and Human Services, 2013).

Administrative safeguards cover the security management process. Designated security officials are tasked with identifying and analysing threats to ePHI and with setting up appropriate security measures that mitigate malicious attacks and data mining. Judging by the role of the individual requesting access, security rules are implemented by those responsible for Information Access Management (IAM), who grants access on a need-to-know basis (role-based access). There is a chain of command amongst professionals stressing that only certain responsible individuals are granted access to sensitive data sources, thus preventing misuse or negligence. This also requires the security officials and IAM to design and update workforce training and management that promote and accommodate awareness of the regulations and consequences of non-compliance (U.S. Department of Health and Human Services, 2013). It is therefore important to secure for example the mHealth application when designing it and only ask for the personal data that is needed (by default). This can mitigate the risks of data breaches.

Administrative safeguards should also minimise the presence of ‘individually identifiable health information’, “that is, data that can be pinned to a particular individual, leading to a rise in direct

phishing attempts by malicious third parties". This data includes demographic data that relates to the individual's past, present or future physical or mental health condition (HIMSS, 2017).

2.2.2 Security of data stored on mobile devices (local storage/cloud)

There are two distinct ways in which mHealth apps can store private data and the developers should decide to allow their apps to do so. The data can either be stored locally on the device or can be sent to a secure external resource (or cloud). The pros and cons of using either or a combination of these two storage practices have to be weighed up by developers and consumers.

The pros and cons of the various storage method (local or cloud) are presented in Table 2.

Table 2: Pros and cons local and cloud storage

	Local storage	Cloud storage
Pros	The easiest, fastest and simplest option, local storage is a cheap and efficient use of already existing storage hardware offered by a device. Local storage is very fast and does not require connectivity (Hedge, 2016).	The data cannot be lost or stolen when the device's security or functionality has been compromised. The data can be accessed from any device, provided that the user has been sufficiently authenticated (Staimer, 2012).
Cons	Targeted attacks and viruses that can override the security of a device and access the sensitive data using the device's own digital signature. Physical or mechanical failures can make this data inaccessible to the user but vulnerable to savvy specialists, who can still extract the data whilst repairing or hacking the device. The user may believe the data has been lost or destroyed (Hedge, 2016).	It has been demonstrated that data stored in the cloud can be infiltrated by hackers (external) and internal parties (leaks) (Staimer, 2012).

Cloud storage is better than local storage at handling large-scale data handling issues such as storage; it is also better at permitting the expansion of services and data migration, as all data can be maintained centrally as opposed to being dispersed across many independent devices (Staimer, 2012). Data storage is usually a service that charges for the additional storage. Cloud-storage requires connection to the internet (Zhang, 2017). As a result, internal administrators, such as IT departments, lose control over the data stored on third-party servers.

Choosing the appropriate method for storage will depend on the requirements of the service being provided. If collaboration and file-sharing abilities are central requirements, then cloud-based storage is appropriate. Small businesses with little revenue should opt for local storage. If data security and costs are the biggest internal concerns, then a cloud-storage can be created on an internally maintained resource as a compromise (Tom, 2014).

With the emergence of health-related apps and the sensitive data they collect and arose the phenomenon that private health data has, to some extent, slipped out of the control of medical institutions. This data has been interspersed across mobile devices and private companies over which medical institutions have little or no control. It is, therefore, critically important that sensitive information stored locally and in the cloud is secure and protected and that the companies handling the data ensure privacy and confidentiality. However, all of these developments have shifted responsibility in terms of data protection onto private individuals and companies, all of whom differ in their awareness of the associated risks. This shift and the international nature of today's development and storage mechanisms have created the need for a cross-border legal framework, one that requires (inter-) governmental intervention. Security mechanisms on mobile devices include password protection, malware scanners, firewall services, encryption utilities, and secure transfer protocols. In addition, software installation from unknown sources should be prohibited and a reluctance to share information on unsecured networks should be encouraged.

Example of storage (Apple HealthKit)

The Apple HealthKit, for example, includes a number of standard security features. HealthKit transfers data from applications to the storage on the iPhone or Apple watch and to an encrypted database named the ‘HealthKit Store’. It also has the ability to receive data from other devices and data sources, provided these other devices have a HealthKit companion app to facilitate the transfer. Once synchronised, HealthKit’s app allows users to manage their health and fitness data themselves and edit sharing permissions for each type of data. This puts some of the administrative, physical, and technological safeguards in relation to data security in the hands of the end-users. Apple HealthKit grants ‘fine-grained’ control of users over their information and how it is shared (Apple, 2013). Fine-grained control is that every data item has its own access control, it is commonly used for cloud computing (Xinfeng, Bakh, 2015). Information leakage is avoided by allowing users to grant different access rights to different data. However, it is never clear whether the app has denied permission for someone to read the data. As an additional precaution, HealthKit data is kept only on local storage (on the user’s device) and this data becomes encrypted whenever the device becomes locked. In chapter 4.1.2.2 more details will be given concerning Apple HealthKit.

Apple, in its developer documentation, states that it provides the following administrative safeguards in relation to HealthKit:

- The app may not use information gained through the use of the HealthKit framework for advertising or similar services.
- A developer or other administrator must not disclose any information gained through HealthKit to a third party without express permission from the user. Even with permission, information can be shared with a third party only if that third party is also providing a health or fitness service to the user.
- Developers and administrators are not allowed to sell information received through the HealthKit store to commercial platforms or to those that are reselling the information.
- If the user consents, Apple may share an end-user's HealthKit data with a third party for medical research.
- The app must clearly disclose to the user how the app will make use of their HealthKit data (Apple, 2013).

2.2.3 Security in connections

The transmission of data from one device to another or to a server for storage also implies that, at certain times, data has left the security of the user's device and has been transmitted to a relatively unknown location (Kumar, Lee, 2012). When, for example, a mobile health app allows users to share health performance records with each other (say, two friends training together), this information would go through some kind of service linked to the internet or more directly through a Bluetooth connection. No-one can be 100% sure that the connection between these two devices is secure. Bluetooth communications can be intercepted and the security of the service which transfers information over the open internet may be questionable. Furthermore, recent hacking and leakage scandals that affected some of the world's largest companies and government institutions has tarnished the credibility of even the most advanced data security systems. So the moment that data leaves a device for whatever reason, it becomes subject to a whole host of potential threats.

Apple HealthKit facilitates the handling of data transaction to and from apps by digitally signing the sample data created, allowing other apps to confirm the safe storage of such data. By making use of cryptographic message syntax (CMS), the digital signature provides a technological safeguard that validates data and the device on which it is being created (Apple, 2013). Through these measures, data transferal can be made much safer between apps and approved devices.

2.2.4 Cybersecurity threats

In this age of digital information and communication, cyber security threats are an unfortunate reality. Attacks on critical infrastructure and vital assets of public interest, including those used in relation to healthcare, are on the rise and pose a serious threat to the health and well-being of the general public. The security risks to the data obtained, stored, and transmitted on mobile devices have been highlighted by many studies.

For example, malware infections are a growing problem. Malicious software may exploit application vulnerability or use social-engineering techniques to trick the user and install itself on a mobile device. The installed malicious software on the device can then obtain stored sensitive health information and send it to an entity that the user of the device did not intend. More often than not, the owner of the host device will have no idea their data has been copied and used as a bargaining chip for a financial exchange. It is important to emphasise the fact that mobile devices are vulnerable to unauthorised usage or physical theft in case they left unattended, which could lead to the disclosure of health information or lack of availability of the medical application.

Recently, a spate of cyber-attacks on hospitals put personal health information and the operation of hospitals under threat. On the 12th of May 2017, hospitals around the world were hit by a ransomware attack. Software that had exploited technology leaked for the US National Security Agency (NSA), it denied access to files stored on machines and servers, cancelled surgical operations, diverted ambulances, and blocked access to patient records. Although Microsoft quickly released a patch through a software update to fix the vulnerability exploited by 'WanaCrypt0r 2.0', its real name, older computers that had not received the update were still at risk (Guardian, 2017). The software used, called WannaCry, blocked access to data and demanded a $300 transaction in bitcoins for those wishing to regain access to their data. Government agencies, and consequently the media, urged individuals who required access to the data not to give into the demand for ransom, as it began emerging that is exactly what some people had begun doing. In the United Kingdom alone, 16 hospitals were shut down temporarily (Brandom, 2017). This particular attack also affected energy sectors, transportation, and shipping and telecommunications; it infected over 230,000 computers in 150 countries. This attack could happen again in the future and it is, therefore, imperative that all sectors ensure state-of-the-art security practices and safeguards (Ehrenfeld, 2017).

2.3 Privacy and confidentiality

Although most people assume that privacy and confidentiality mean the same thing, an important distinction should be made between the two.

Cohn (2006) gives a clear definition of the difference in meaning between privacy and confidentiality:

> Health information privacy is an individual's right to control the acquisition, uses, or disclosures of his or her identifiable health data. Confidentiality, which is closely related, refers to the obligations of those who receive information to respect the privacy interests of those to whom the data relate.

In the health information context therefore, 'privacy' involves the end-user's primary concerns, whereas confidentiality focuses are on the responsibility of those institutions and private organisations entrusted to receive, store, and process private data. As the focus is on Personal EHR on mobile devices detailed information will be given in chapter 2.4.

2.4 mHealth (definition)

The WHO (2011) defines mHealth as 'the practice of medicine and public health supported by mobile devices such as mobile phones, patient monitoring devices, personal digital assistants and other wireless devices' (WHO, 2011).

2.4.1 mHealth market

Research2Guidance reported that, from early 2013, there were about 97,000 mHealth apps across 62 app stores and that this industry had been booming ever since (Aitken & Gauntlett, 2013). MarketsandMarkets released a report stating that the global mHealth market is predicted to grow from $6.21 billion in revenue in 2013 to $23.49 billion by 2018 at a 30.5% compound annual growth rate (CAGR) over the five-year-period from 2013 to 2018 (MarketsandMarkets, 2014).

In 2013, Apple calculated that for its IOS operating system for Apple mobile devices, it had more than 43,000 medical, pharmaceutical, and fitness related apps in its app store, while Google Android had around 16,000 apps.

Of the 43,000+ iOS apps:

- 16,275 were consumer- or patient-oriented or they were developed for healthcare providers.
- 5,095 apps had the capability to capture data entered by users.
- 395 apps could communicate with healthcare providers or share data across social networks.
- 159 apps could connect with external sensors.
- Fewer than 50 could measure vital signs.

The dominant categories and their portion of the market of the different mHealth apps can be seen on the pie-chart in Figure 1. Depending on the type of personal information being provided (for example, information that can link personal data to a single person such as an official name), the

disease & treatment management group has the most sensitive data that would-be hackers are looking for.

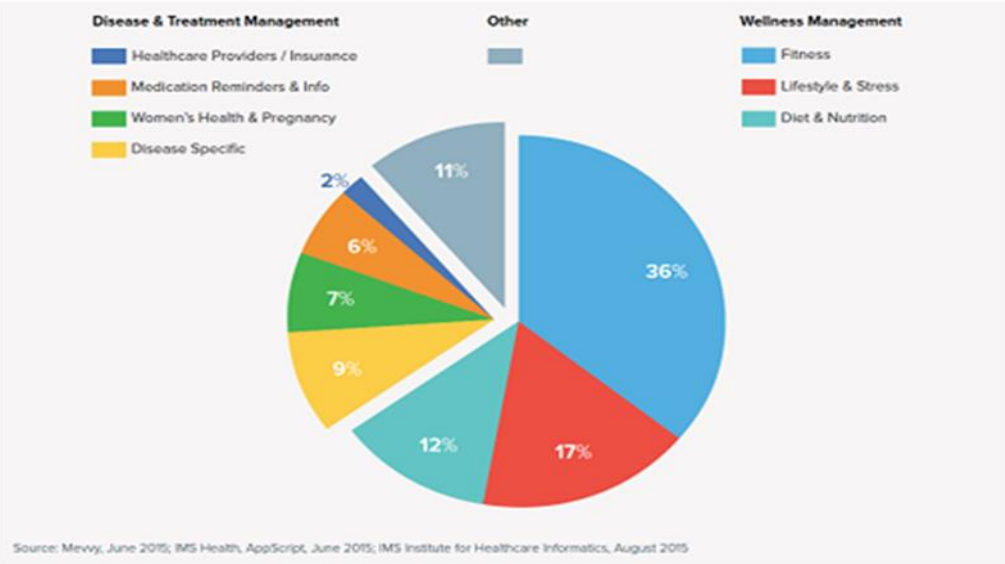


Figure 1: mHealth apps by category 2015

Source: Mevy, June 2015, IMS Institute for Healthcare Informatics

Mobile Market

Most applications that are used for mobile health are on the IOS or Android operating system (see Figure 2 and Table 3). These are the two biggest mobile platforms in the smartphone market. Therefore, the focus of this study is on applications/API on IOS and Android because they represent the most-used and the most-popular mobile devices.

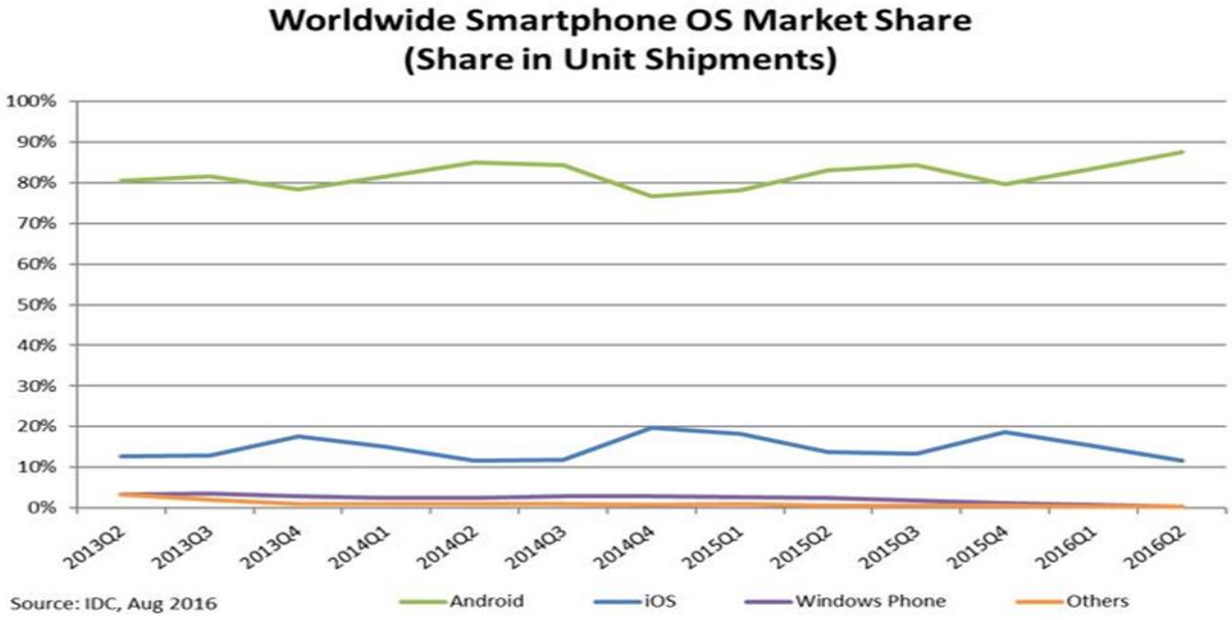


Figure 2: Market Share Smartphones

Table 3: Percentage of Market Share

Period	Android	iOS	Windows	Others
2015Q3	84.3%	13.4%	1.8%	0.5%
2015Q4	79.6%	18.6%	1.2%	0.5%
2016Q1	83.4%	15.4%	0.8%	0.4%
2016Q2	87.6%	11.7%	0.4%	0.3%

The Cisco Visual Networking Index predicted that by 2019, there would be almost 1.5 mobile devices per capita globally. The popularity and mobility of smartphones and tablets make them lucrative platforms for healthcare practices. They demonstrate the ability to be pervasive and user-friendly; they also have fast growing computational capabilities, built-in sensors, and fast-growing connectivity.

2.4.2 mHealth applications and wireless connections

mHealth applications can also be connected with sensing apps like Bluetooth to collect data from health sensor to mobile devices. The body area network (BAN) allows wearable devices, for example, a watch or glasses, to send in personal data about an individual's health and fitness to his or her devices. Readings may include heartrate or blood-sugar levels. By using the measures demonstrated by Apple's HealthKit, for example, digital signatures can validate the data being transferred and simultaneously encrypt it to protect it from being hacked by outsiders.

It is, therefore, important that sensitive data is encrypted before it is communicated via mobile devices through the internet. Users need to know what is stated in privacy policies. App developers might have agreements where they share personal data with for example other parties.

2.4.3 Malicious attack

There are many threats to mobile data that are increasing in number and sophistication. One such threat is a remote access tool, which is software designed to access a computer or other device and their data storage remotely. There are genuine uses for these applications; however, when they are used for malicious purposes they are known as remote access Trojans or RATs. RATs have the potential to simultaneously access the data of multiple devices and have, in the past, targeted large groups of people (Infosec, 2014). There are trading networks dealing in data with the intent of stealing private media from a targeted individual's device. This can be achieved by accessing the device's local data or by using the devices stored log-in credentials or access cloud-based backup services on a mobile phone. In 2013, Google reported an average of 5,768 malware attacks on its

Android OS in just half a year. The number of recognised vulnerabilities for iOS-based devices increased a massive 82% in 2013 (CSO, 2014).

Data collectors can go as far as scouring Facebook and other cloud-based resources to dig for any information that could be sold or that is useful; they have also targeted public record services or credit-reporting agencies. Malicious data gatherers go so far as to set up false Facebook or Skype accounts in an attempt to get as close to as many would-be victims as possible. Information on these sites contain clues that might even assist hackers in answering security-question challenges, thus enabling them to gain full control over accounts. RATs, phishing, account recovery, and password reset procedures are the most common methods of getting into networks of personal data (Cubrilovic, 2014). Hence, even though users might have the same devices and applications, one particular user might be a lot more unfortunate than another in terms of his or her data stored on mobile devices being targeted through carelessness.

3 Research methodology

3.1 Research approach

The research reported in this study combined the use of inductive and deductive approaches. Literature was obtained from various credible sources (journals, books, and scientific papers) in order that a greater insight into the development and current state of personal data security could be gained, particularly in terms of eHealth. A number of interviews (qualitative data) took place with professionals in the fields of medical practice, healthcare, and data-security experts, as well as with consumers. A survey was also conducted to obtain quantitative readings reflecting trends in the marketplace. Different stakeholders were targeted in this analysis, and their roles in the industry and the risks they face were defined and discussed. As the kinds of threats they faced emerged, ways to reduce those threats were also investigated by means of information contained in the relevant literature. The findings in the surveys helped to validate the qualitative interviews. An exploratory approach was adopted, which involved the reading of relevant literature, interviews with experts, and an analysis as already mentioned.

In the literature different kind of apps for Apple IOS and Google's Android OS's were scored on the security mechanism that they would at least need to have some security measures. It was clear from the outset that it would not be accurate to analyse one particular app in isolation, because general trends would not emerge from such an analysis. Security reports about apps working on Apple IOS and Google Android were examined, and these gave a good indication of how safe these operating systems were.

3.2 Literature review

The literature review made use of the methodology proposed by Saunders et al (2009).

Parameters

The table below maps the parameters that govern the areas on which the research focused (Mark Saunders, 2009)

Table 4: Parameters research

PARAMETER	NARROW SEARCH	BROADER SEARCH
LANGUAGE:	English (UK, USA)	Dutch, English (UK, USA,)
SUBJECT AREA:	Privacy and Security in mHealth apps	Privacy and Security on mobile devices,

		Privacy and security in mobile applications Personal electronic health records
SECTOR:	Mobile Health Sector	Health, mobile industry
GEOGRAPHICAL AREA:	Netherlands, UK, USA	International
PUBLICATION PERIOD:	Last 5 years	Last 15 years
LITERATURE TYPE:	Scholarly, scientific databases	Internet, publications, journals, books, and research papers

Keywords

The keywords applied in the research were:

- mobile health;
- privacy and security;
- eHealth;
- data storage;
- health applications;
- confidentiality;
- guidelines and standard mobile applications; and
- privacy laws.

3.3 Interview techniques

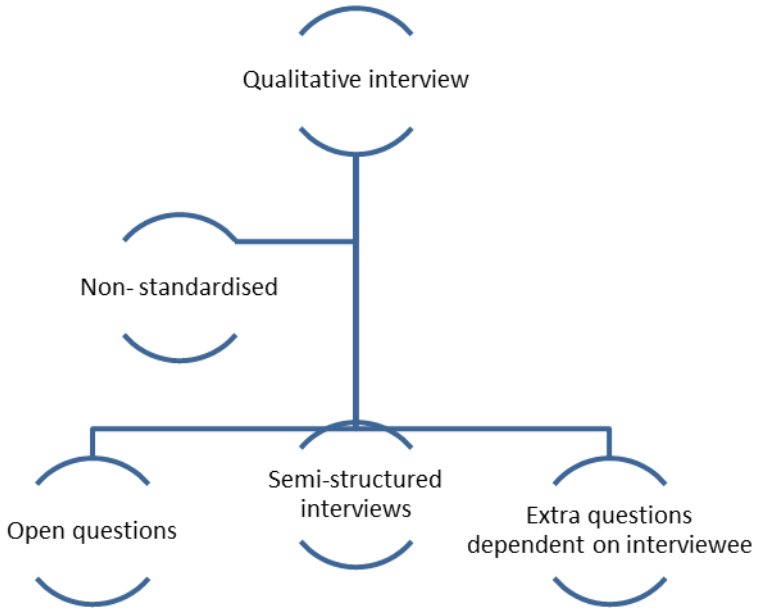


Figure 3: Interview method

Figure 3 illustrates the interview plan. A qualitative interview was carried out and was applied on the basis of combining inductive and deductive approaches. The collection of qualitative data will be applicable. Semi-structured interviews were undertaken in order to discover events or information that might not be clear, thus leading to clarification of the crucial issues involved. The benefit of this interview technique was that it provided structure and enabled the interviewer to give some direction to the unfolding process; structure and specific question were also combined with open questions that gave more insight and depth in regard to the topic. Depending on the interviewee, extra questions were added during the interview to solicit additional information. Interviews were conducted with experts in the health sector and in the area of mobile security and in how users are and should be coping with this issue. A trial interview was conducted with individuals not actually involved in the research in order to see which questions were unclear and what questions needed to be added.

The interview was validated through the application of the technique of listening, summarising, and questioning. This technique enabled the interviewee to evaluate the correctness and completeness of the interviewer's interpretation. Interview reports were written, and interviewees were allowed to read through them and approve them. To verify the data that emerged, the results of the interviews were compared to the results written up in recent relevant literature, to see if these interviews contradicted or agreed with information that had been published.

Interviewees' privacy was respected and their names were anonymised in terms of privacy; knowing this, the interviewees felt more open in terms of sharing information.

3.4 Survey methodology

Ten individuals participated in a test survey and they provided their feedback. The answers that they gave were examined to determine which questions were relevant and which were not. During this process, it was found that there was a need to change and rephrase some questions so that relevant information could be gleaned from the surveys.

A survey was finally conducted which elicited information about consumers' thoughts and fears in regard to health-data security.

4 Research results

The results of the literature review, interviews, and surveys are presented in this chapter and are based on an in-depth analysis of the information that emerged. The results indicate that there is a rising awareness of and concern about potential threats regarding the security of health-related data. All those surveyed and interviewed indicated that they wanted the issues clarified and solutions to be found in relation to the handling of personal electronic health records (EHR) data stored on mobile devices. In section 4.4 of this chapter, a correlation will be made between the methodologies used and the outcomes.

4.1 Literature review

This section discusses what the relevant literature reveals about the privacy and security of personal electronic health records on mobile devices. It is clear that there are both benefits and potential threats to bringing healthcare into the digital world, whereby mobile devices (smartphones and tablets) play a crucial role in patient care. Nowadays, there are numerous mobile health applications that could contribute to self-care, making it less necessary for the patients to go on a regular visit to a general practitioner or hospital. It is therefore important that the reliability of access to personal EHR is assured and that patients can trust that their mobile devices are safe and secure.

In this section, the issue of the benefits and potential threats of personal EHR on mobile devices is clarified. Moreover, the security of current mHealth applications and APIs in the market is made clear. Furthermore, this section recommends guidelines and discusses the legal issues involved regarding personal data protection; finally, an analysis of the results is given. Throughout the discussion, the focus is on the two biggest operating systems in the market—IOS and Android (see Chapter 2.4.1, Figure 2 and Table 3).

4.1.1 Benefits and potential threats of personal EHR on mobile devices

Benefits

The user-friendly touch interface, convenience of availability, and ease of connectivity in relation to mHealth apps are appreciated by the users. mHealth apps enable patients to use their devices to access and update medical records, monitor health statistics, and access prescriptions, thus reducing their reliance on healthcare professionals while at the same time enhancing their connection and interaction with them when required. Because of this, the link has been established between the use of mHealth apps and reduction in healthcare costs. A study conducted by the working group of the 2014 study demonstrated the reduction in healthcare costs because of the use of remote monitoring mHealth apps (European Commission, 2014). Smartphones are also used by healthcare professionals

within hospitals to access patients' records, prescribe medications, and access test results (Planchkinova, Andrés, & Chatterjee, 2015).

In Table 5, the benefits discussed in the literature are given, together with the titles of the relevant articles:

Table 5: Benefits of Having Personal EHR on Mobile Devices

Statements	Articles Supporting the Analysis
Bring-Your-Own-Device Approach (BYOD); ease of use and convenience	• (Martinez-Perez, del Torre-Diez, Lopez-Coronado, 2015) • (Yang, 2016) • (Planchkinova, Andrés, & Chatterjee, 2015)
mHealth applications can be used from a distance, at any time and in any place.	• (Adhikari, Richards, & Scott, 2014)
Health care providers can manage their patients' health remotely (telemedicine).	• (Adhikari, Richards, & Scott, 2014)
mHealth apps can improve patients' health. (access and updating medical records and monitoring health statics).	• (Adhikari, Richards, & Scott, 2014) • (European Commission, 2014)
Apps can connect people in different locations while reducing costs and frequency of visits, both with GPs and with specialists.	• (Adhikari, Richards, & Scott, 2014) • (European Commission, 2014)
mHealth apps can improve the availability and helpfulness and affordability of healthcare for patients.	• (Adhikari, Richards, & Scott, 2014)

Potential threats

Dealing with personal sensitive data necessitates making privacy and security requirements a requirement; however, this is not always the case. It is well-established that many health apps create security and privacy problems because not enough checks and balances have been put in place. The conceptual weaknesses of mobile operating systems, the poor programming of the apps, insecure transmission methods, and not enough mechanisms to prevent developers selling on personal data themselves have created loopholes for malicious third-parties (Mense, Urbauer, Wahl, & Sauerman, 2016). Security and privacy concerns have grown in recent years due to the increased occurrences of

security incidences such as database breaches, data ransom, device hacking, and online privacy leakage (Yang, 2016).

Perez' research (2016) specified that a security assessment had identified the potential threats of mHealth apps that need to be secured to protect mobile apps. This research was conducted in 2016 and was supported by the OWASP Mobile Security Project. In Figure 4, the vulnerabilities which are described in the paper can be seen; these vulnerabilities need to be considered before creating mHealth applications (Perez Morera, 2016). Perez (2016) has described the ten vulnerable threats that might expose the personal sensitive data of users as follows:

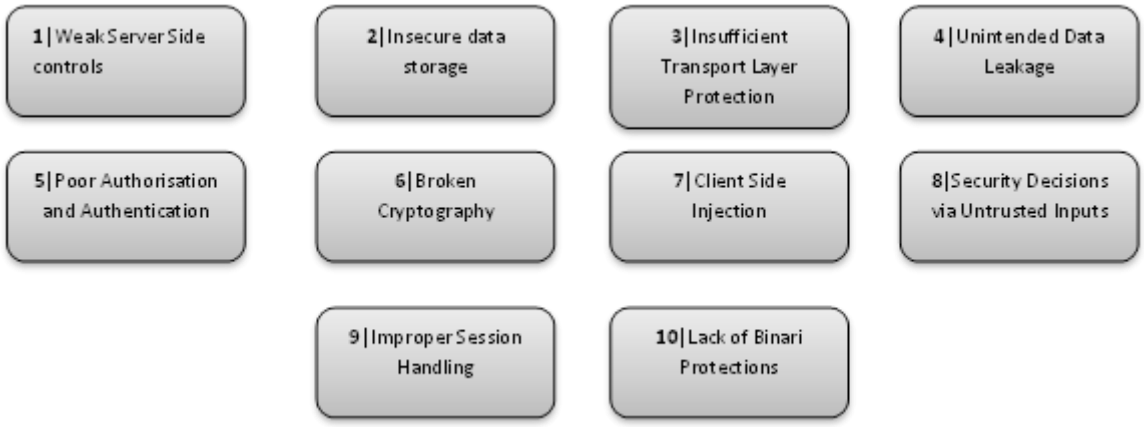


Figure 4: Potential vulnerabilities to consider

Source: (Perez Morera, 2016)

A study was conducted during a six-month assessment of certified mHealth apps in the United Kingdom by the National Health Security (NHS) Health Apps Library. The outcome of these results was that 89% out of a total of 79 certified apps transmitted information to online services and there was no encryption in the transport of data. Twenty percent of the apps did not reflect the fact that there was a privacy policy in place and 67% reflected the fact that there was some form of policy in place (Huckvale, Prieto, Tilney, Benghozi, & Car, 2015). These apps were certified by the NHS Apps Library in the UK and yet not everything was done to ensure that the transport of medical data on mobile apps was secure. Tables 6 and 7 present the results of the assessment.

Table 6: Privacy policy disclosures

Policy	All apps, n = 79 (%)	Apps collecting data		Apps transmitting data	
		Any data, n = 70 (%)	Personal or sensitive data[a], n = 59 (%)	Any data, n = 70 (%)	Personal or sensitive data[a], n = 38 (%)
Privacy disclosure available	53 (67 %)	50 (71 %)	43 (73 %)	49 (70 %)	31 (82 %)
In-app privacy policy	22 (28 %)	22 (31 %)	21 (36 %)	22 (31 %)	15 (39 %)
Other privacy policy	48 (61 %)	45 (64 %)	38 (64 %)	44 (63 %)	29 (76 %)
Policy mentions app	8 (10 %)	8 (11 %)	5 (8 %)	8 (11 %)	5 (13 %)
Advertising policy	3 (4 %)	3 (4 %)	3 (5 %)	3 (4 %)	3 (8 %)
No privacy disclosure	26 (33 %)	20 (29 %)	16 (27 %)	21 (30 %)	7 (18 %)
In-app clinical disclaimer	36 (46 %)	32 (46 %)	26 (44 %)	33 (47 %)	13 (34 %)

[a]Incorporates strong personal identifiers, health-related information and other sensitive information

Table 7: Security vulnerabilities affecting data storage and transmission

Security vulnerability class [49]	Type	All apps, n = 79 (%)
Insecure data storage	Unencrypted data storage (of any data)	73 (92 %)
	Unencrypted username/password	8 (10 %)
	Unencrypted personal or sensitive information[a]	42 (53 %)
Insufficient transport layer protection	Identifying information sent without encryption[b]	23 (29 %)
	Sensitive information sent without encryption	6 (8 %)
Unintended data leakage	Username/password captured in network cache or log	2 (3 %)
	Health-related information sent to third parties	8 (10 %)
	Fixed device identifier used as user identifier	9 (11 %)
Weak server-side controls	Unencrypted access to server-side API	16 (20 %)
	Access to user data without authorization	2 (3 %)

[a]Excluding username and password; [b]considering strong identifiers only

Source: (Huckvale, Prieto, Tilney, Benghozi, & Car, 2015)

In addition, the Appfail report from the Norwegian Consumer Council in 2016 gives the result of an analysis carried out in relation to the privacy policies of mobile applications. The results make it clear that normal applications such as Snapchat do not allow for reasonable notice to be given in advance of possible vulnerabilities and do not convey vital information if and when privacy policies have been subject to change. In other words, changes to privacy policies are made without users being informed. Health applications like Endomondo, Runkeeper, and MyFitnessPal do not give notice in advance of alterations to the terms and conditions (Radet, 2016). In this case, even a sophisticated user who understands data-security issues might be caught aware by changes to the original terms and conditions to which they agreed.

Finally, in Table 8, there is a list of potential threats that were mentioned during the literature review; they are listed below, together with the sources:

Table 8: Threats to Personal EHR on Mobile Devices

Statements	Articles Supporting the Analysis
Clinicians and patients are adopting mobile technologies faster than providers can protect security and privacy. That is a significant problem	• (Martinez-Perez, del Torre-Diez, Lopez-Coronado, 2015)
User unawareness of the privacy and security aspects of mobile applications that they use in their daily activity; thereby patients do not secure their own device with proper authentication (passwords or fingerprints).	• (Martinez-Perez, del Torre-Diez, Lopez-Coronado, 2015) • (Adhikari, Richards, & Scott, 2014)
Poor authorisation and authentication	• (Adhikari, Richards, & Scott, 2014) • (Martinez-Perez, del Torre-Diez, Lopez-Coronado, 2015)
Lack of proper privacy policies for users	• (Huckvale, Prieto, Tilney, Benghozi, & Car, 2015) • (Adhikari, Richards, & Scott, 2014) • (Martinez-Perez, del Torre-Diez, Lopez-Coronado, 2015)
Lack of regulation on the mobile market and lack of standardisation of security issues and app development guidelines	• (Planchkinova, Andrés, & Chatterjee, 2015) • (Adhikari, Richards, & Scott, 2014)
Incorrect medical advice provided by mHealth can be harmful if users rely on it.	• (Adhikari, Richards, & Scott, 2014)
Data poorly managed and not encrypted when it is send; therefore, other parties can get access to it; insufficient security measures in place to safeguard consumers' sensitive data	• (Mense, Urbauer, Wahl, & Sauerman, 2016) • (Huckvale, Prieto, Tilney, Benghozi, & Car, 2015) • (Adhikari, Richards, & Scott, 2014)
Medical identity theft (outsider may alter false entries and you may receive false medical treatment that may cause fatalities.	• (Adhikari, Richards, & Scott, 2014)
Information sent to third parties	• (Dehling, Gao, Schneider, & Sunyaev, 2015) • (NHS, 2015) • (Adhikari, Richards, & Scott, 2014)

4.1.2 Security mHealth apps and APIs

4.1.2.1 mHealth apps

In 2013, it was discovered that information for users was collected by apps that were poorly protected (did not have authentication measures and other security mechanisms). However, out of

43 health and fitness apps considered for the study, 74% of the free apps did provide a privacy policy which was displayed either by the app or on the developer's website (60% of the paid apps did). Only one-quarter of the free apps and just under half of the paid apps informed end-users about security measures. Of all the apps tested, only a few of the paid apps encrypted the data being collected from users. Encryption of user data is an integral part of preventing unauthorised intruders from being able to intercept and interpret information being accessed into something they can use or sell (Adhikari, Richards, & Scott, 2014)).

In 2015, it was discovered that out of the 24,405 health-related apps tested (iOS; 21,953; Android; 2452) there was an absence or scarcity of ratings for 81.36% (17,860/21,953) of iOS and 76.14% (1867/2452) of Android apps. This indicates that less than a quarter of mHealth apps are in widespread use and most of those apps (95.63%, 17,193/17,979; of apps) posed at least some potential threat to information security and infringed privacy. There were 11.67% (2098/17,979) of apps that scored the highest assessments of potential damage (Dehling, Gao, Schneider, & Sunyaev, 2015)The research that is discussed here applied a clustering approach, whereby app-tagging created a description that is machine readable. The cluster assessment that was conducted showed results that are presented based on the specification of health information, leaks, change, loss, and the value of information to third parties.

On the mHealth market, iOS and Android also provide application programming interfaces (APIs [1]) for developers that can create EHR data apps. An API is a set of routines, protocol, and tools for building software, specifying how software components should interact (API Academy). An app developer can choose to create his or her own app, or use an API that already provides the building blocks to develop a pre-existing template (although the app developer still needs to write his or her own piece of code for their app). Flanders (2015) states that APIs allow one piece of software that makes use of the functionality or data available to another; this allows developers to access the functionality of other software modules through well-defined data structures.

4.1.2.2 APIs

Apple HealthKit

With the Apple HealthKit, it is possible to share health and fitness data with other apps while maintaining the user's privacy and control over that data (Apple Inc, 2016).

[1] API stands for application program interface and is a set of routines, protocols, and tools for building software applications. A solid API makes it easy to develop a program by providing the building blocks that will be developed by the programmer http://www.apiacademy.co/resources/api-strategy-lesson-101-what-is-an-api/.

The advantage of using this API is that a developer will save time in developing mHealth applications in IOS. Apple states that HealthKit allows the developer to focus on implementing only the aspects that are of most interest to the users. For developers, it is easy to interact with the different apps a user might be using.

HealthKit data is stored only on the user's device. To protect the data, HealthKit is encrypted when the device is locked. It can only be accessed by an authorised app. HealthKit makes it possible for users to have control over their own data. Apple is obligated as app provider to deliver a privacy and security policy for the HealthKit framework. Apple guides in delivering a privacy policy that complies to personal health record model for non-HIPAA apps or the HIPAA model.

Apple HealthKit gives users granular control over the health data that other applications can access. Granular control in the authorisation control means, a user can decide which application can see which data (in terms of reading and writing permission). The user can also change this permission (Apple Inc, 2016).

The advantages Apple describes in HealthKit are:

- the separation of data collection, processing, and the socialisation of data;
- automatic data-sharing between apps is enabled. Developers do not need to write codes for this anymore. Users do not need to set up connections between their apps and can, for example, choose a certain app within HealthKit for heartrate and another one for nutrition and;
- the availability of a rich set of data and context whereby developers with anonymous statistics can improve access, service, and security. The app developer is then also aware of the wishes and needs of the users in the development of mHealth applications.

Google Fit (Android)

Google Fit cannot ensure the security of personal data that will be stored and accessed through this API. The terms and conditions describe the fact that Google Fit is not a medical device. Google Fit does not make it compulsory to conform to the HIPAA law and does not apply this regulation (Google, 2016) Google does make sure, however, that personal data is protected by using the following mechanisms:

- Communication with the service occurs through a secure connection. It is not possible to communicate with the service through insecure connections and Google Fit cannot be used without a Google Account.

- Delete History feature: Users can decide when and what information to wipe from all storage locations at will.
- Third-party connections: Apps can be approved by the end-user, a process which will communicate health data to and from the Google Fit app. This is the point where Google loses some control over the data, as third-party apps have their own set of principles and end-user agreements.

Samsung S Health

Samsung S Health has a security mechanism whereby this app assures the security of this API. The SDK (Software Development Kit) permits its technologies to do the following:

- combine predefined data types with custom data type;
- normalise data between devices via transparent data layer;
- import and export of data and;
- transform data to a manageable format for analysis of small and big data (Samsung, 2016)

This API is integrated with Samsung devices and sensors for mHealth applications; in Figure 5, the layers are illustrated whereby it can be seen how third-party apps and S Health are connected on their devices within the different layer

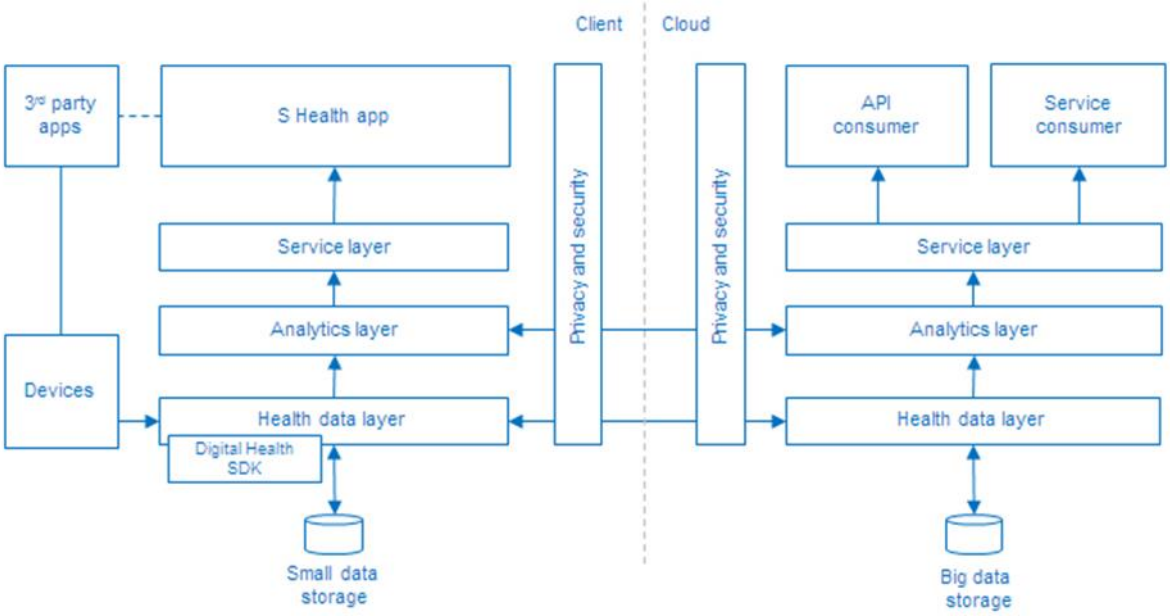


Figure 5: Conceptual System Architecture S Health

Source: (Samsung, 2016)

In terms of security, the API Samsung applies is the Samsung Knox Security solution. The Samsung Knox Security solution provides a set of communication methods whereby apps share their data with each other. This security framework makes sure that there is no communication between the

enterprise apps and user apps in ensuring that personal sensitive data will not be leaked to third parties that cannot be trusted. The main difference between user- and enterprise apps is that enterprise apps are used by the industry in question, whereas user apps cater to end-users, who are private individuals. Enterprise apps are created to become a mobile interface for what is essentially an already existing system in use by the enterprise. This is done through the use of advanced Mobile Enterprise Application Platforms (MEAPs). The security requirements for user apps are considered to be less rigorous than those for enterprises by developers, because enterprise developers adhere to strict client-requirements in addition to existing regulations (Samsung Electronics Co. Ltd, 2016).

4.1.3 Guidelines: personal data protection

Based on the potential threats mentioned in Chapter 4.1.1, authors like Adhikari (2014) and Perez (2016) also provide solutions to ensure that mobile data is secured. Based on this, an identification process and comparative analysis of 20 mHealth applications has been carried out by Adhikari's (2014). The questions to test the identification process are as follows:

- Does the mHealth application ask for user registration?
- Does the mHealth application ask for authentication?
- Can consumers delete any personal information completely?
- Where is data stored (locally or in a cloud)?
- Is the personal data of consumers shared with third parties or advertisers?
- Are consumers informed about any data and security measures?
- Is there a privacy policy? (Adhikari, Richards, & Scott, 2014).

These were the guidelines presented by Adhikari (2014) as being necessary to protect personal data; Adhikari (2014) also advises that the two main actors involved in mHealth applications—consumers (users) and applications developers, need to become more aware of potential threats and of required security measures. Thus both groups can contribute to more safety in mHealth applications. These guidelines are shown in Table 9. Chapter 5 provides a more detailed description of the role these actors can play in the privacy and security process of mHealth applications.

Table 9: Adhikari's guidelines: consumers and developers

Consumer (User)	Application developers
Research the app before downloading it.	Sensitive consumers' information should always be stored encrypted. So that attackers cannot simply retrieve this data.

Try to use apps without entering personal information if permitted.	Include user authentication.
Look for user reviews and the privacy policy of an app, either through the app store or online.	Minimise sharing information with third parties or advertisers
Remove data when usage stops. This may prevent unauthorised use of stored data when consumers no longer use the apps.	Apps should allow consumers' to delete their personal information completely.
Give feedback on product: Users' feedback on features and privacy policy.	Provide user whit information about the implementation of security measures and authentication and what how/where their data is stored.

Source: (Adhikari, Richards, & Scott, 2014)

Taxonomy mHealth

In mHealth applications, personal sensitive data is stored and transported, unlike the usual applications on mobile devices. Thus creating a unified taxonomy of mHealth apps is useful and necessary to make classifications that capture the essence of the data required to address privacy and security issues. In assuring that app developers will understand which dimensions are important for mHealth applications and that they may differ from other types of mobile applications. To get a better understanding of the privacy and security concerns in relation to mHealth applications Planchkinova (2015) created the taxonomy below which reflects three important aspects: the app, security, and the privacy dimension (see Figure 6). The threats in the dimension are as follows:

- for privacy: identity, access, and disclosure threats;
- for security issues: Authorization and authentication, integrity, and accountability, ease of use, and availability;
- confidentiality management and physical security (Planchkinova, Andrés, & Chatterjee, 2015).

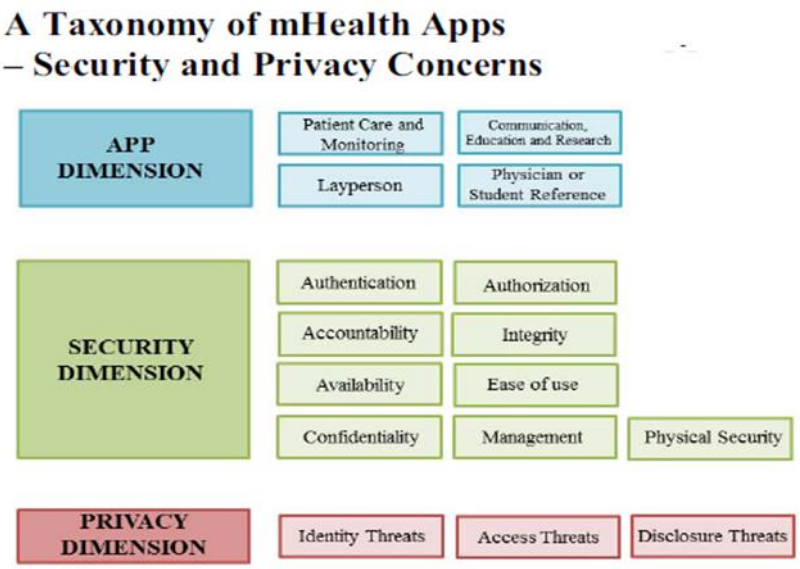


Figure 6: Taxonomy of mHealth apps

Source: (Planchkinova, Andrés, & Chatterjee, 2015)

Physicians and other healthcare providers may not always have access to the resources (including financial), infrastructure, and expertise required to establish fail-safe defence systems (World Medical Association, 2016). This stresses the need for appropriate public as well as private bodies to support them in overcoming these limitations. This will also entail responsible practices with regard to how these apps are developed and marketed (World Medical Association, 2016)

4.1.4 Legal issues in regard to personal data protection

In this section, the laws that contribute to the protection of personal information of users (citizens) will be discussed. In terms of laws in relation to digital security, the focus will be on HIPAA law in the US and European data protection laws.

The HIPAA Protection Law

HIPAA, the Health Insurance Portability and Accountability Act, sets the standard for protecting sensitive patient data. Any company that deals with protected health information (PHI) must ensure that all the required physical, network, and process security measures are in place and followed (U.S. Department of Health and Human Services, 2016).

According to the report of the United States Department of Health and Human Service, released in June 2016, there are challenges that could harm the safety and privacy of electronic health information. The focus was on the HIPAA law that is applicable in the US. The challenges in the applying the HIPAA rule that described are:

- new types of entities that share, collect, and use health information that is not regulated by the HIPAA law;
- individuals might not know or have only a limited knowledge about when data about their health is protected by law and when it is not;
- the collection of health information from more than one source without the imposition of consistent security standards, actions that might pose cybersecurity threats; and
- a lack of understanding as to which regulations may hinder the growth of the economy and the progress being made in creating beneficial products that could support generating better health, improved spending of resources, and healthier people (U.S. Department of Health and Human Services, 2016).

The report of the HIPAA law that was issued by the Department of Health and Human Services declared that the HIPAA law is not applicable to all organisations, but that it covers certain entities and their business associates. Organisations that do not fall under the regulation of the HIPAA are not obliged to follow the regulations governing the protection of privacy and security.

Furthermore, it is stated that HIPAA Security rule demands that covered entities[2] perform a security assessment that identifies and mitigates risks to the confidentiality, integrity, and availability of the personal data of patients. As earlier described in chapter 2.2.1, specifics on physical, technical, and administrative safeguards need to be in place. This implies that there are virtually no or few legal frameworks in place to prevent the vast majority of app development corporations from divulging or even selling sensitive private healthcare information. Companies can encrypt data, but the data can still be accessible and distributable by those companies or, potentially, by individual employees. Current measures in place are: internal policies and procedures, workstation security measures, device controls, technical access controls, audit control, integrity authentication mechanisms related to a person or an organisation (U.S. Department of Health and Human Services, 2016).

A legal issue related to these apps having control over such data lies in the fact that mobile health apps do not qualify as being non-covered entities. This means that app developers do not fall under the Health Insurance Portability and Accountability Act (HIPAA[3]) (U.S. Department of Health and Human Services, 2016). This being the case, developers do not necessarily have to conform to

[2] Covered entities "applies to health plans, health care clearinghouses and health care providers conducting certain electronic transactions' (European Parliament and Council of European Union, 2016). For detailed information about what health plans, healthcare clearinghouses, and healthcare providers are see the Glossary
[3] HIPAA is the acronym for the Health Insurance Portability and Accountability Act that was passed by the US Congress in 1996 http://www.dhcs.ca.gov/formsandpubs/laws/hipaa/Pages/1.00WhatisHIPAA.aspx.

industry-wide standards for healthcare information that help to ensure privacy and security protections appropriate for the creation, storage, mobility, and exchange of sensitive data.

The law that applies to entities that are both covered and non-covered entities is the Federal Trade Commission Act (Section 5), which is applied when an organisation misleads consumers to sign on a portal or applications to enter medical information that is subsequently used to sell to other third parties (U.S. Department of Health and Human Services, 2016). This is supported by the report by the FTC, which reveals that a lot of companies use medical information for purposes which were not intended. One example was a medical billing system that was giving information to pharmacies and insurance companies during the signing-in process. Such companies need to make sure that they have systems in place to ensure that the consumer data that they gather is safe and secure.

European Data Protection Law

The European Parliament and the Council of the European Union have released a new data protection law that ensures that there is adequate regulation in place in relation to the processing of personal data. These are laws that contribute to a secure environment and which ensure the privacy and confidentiality of data. A study of EU data regulation (discussion below) indicates that some articles in the law specifically mention what and who can be protected.

To give an indication of what laws can do to enhance the security of personal EHR of medical data and the provision of confidentiality whereby users or patients can granularly have more control over their data will be summarised.

The key points in this regulation (European Parliament and the Council of the European Union, 2016)are summarised below:

- There needs to be transparent information and communication for the user to exercise his or her rights in terms of data protection (mentioned as data subject ‘Article 12’).
- The consumer shall have the right to demand from the controller the erasure of personal data concerning him or her without any delay and, in such a case, the controller can require that the app developer also deletes it without delay (‘Article 16’).
- The consumer should be able to restrict the processing for the accuracy of personal data and enabling the app developer to verify and machine-readable format whereby consumer have the right to know how and which data is transmitted. (‘Articles 18 &20’).
- Data protection by design and default: Developing security mechanism before an application is designed and making sure that data that is needed for the mHealth application to function is asked. Appropriate technical and organisational measures should be put in place (such as

pseudonymising), which are designed to implement the principle of data minimisation. Additional measures, such as appropriate technical and organisational measures should also be drafted that will mean that, by default, only personal data which is needed for processing is processed ('Article 25') ((European Parliament and the Council of the European Union, 2016)

These were some of the regulations that will support technologies to improve the privacy and security of personal data and enhance the confidentiality of users granularly taking control over their data.

The existence of such European laws contributes to the enforcement in applying certain security measures in securing personal sensitive information. The laws give the users the right to have granular control over such information. The users have the right to receive a machine-readable format whereby they know exactly which information the supplier (the app developer) has.

4.1.5 Analysis

Out of this methodology, an analysis can be made as to what the benefits, threats, and the solutions are in using mHealth applications:

The *benefits* of applying mHealth applications are:

- They are easy to use.
- They can be used from a distance and at any place and time.
- Medical records can be updated and health statistics can be monitored from a remote location.
- They improve the availability, effectiveness, and affordability of health care for patients.
- Healthcare costs are reduced.

The Potential t*hreats* of accessing and storing personal electronic health records on mobile devices are:

- The lack of standards and guidelines: there is no market regulation so everyone is free to create an app without the presence of any security or privacy policies on specific mHealth applications.
- A lack of knowledge on the part of the consumer: There is no proper privacy policy whereby the user does not know what he or she has given permission to.
- There is no clarity about where data is stored and shared (whether the storage is in the cloud or lies with third-party sites).

- Data is stored insecurely without encryption.
- There are poor authentication and authorisation controls that, for example, give hackers a greater chance of accessing someone's personal sensitive information.
- Data is shared with third parties.
- There are design/conceptual weaknesses inherent mobile operating systems.

This means that not all security measures adequately address the lack of understanding of what is actually being done with the data that is being collected. Current mHealth applications are, therefore, not fully secured. The NHS in the United Kingdom in chapter 4.1.1 already stated that certified apps transmitted information to services online without any encryption and proper privacy policy.

The threats can be *solved* by:

- Making sure that there are standards and guidelines for mHealth applications that will regulate the certification process and thus regulate the market (Section 5.2, 5.3 contains a more detailed explanation).
- Privacy policies should conform to HIPAA and EU data protection regulations in relation to the enforcement of the laws applicable to these technologies so that mHealth sensitive data can be protected.
- Security by design and default: Security needs to be of paramount importance when the apps are built to form the interface.
- Users of security measures should be specified as should the risks for developers.
- Two-factor authentication and authorisation should be put into place.
- The data transmitted, retrieved, and stored should be encrypted.
- The application of the taxonomy of mHealth should be applied so as to better understand these applications and cover all aspects of mHealth-specific apps.
- Users should be given the ability to control or to delete any personal data completely and immediately.
- Users should be able to receive a machine-readable document summarising the data—what the data is and where it is being stored.
- API frameworks should be used when mHealth applications are created. For example, Apple HealthKit applies the HIPAA regulation for covered entities and for non-HIPAA apps, it applies the Model Privacy Notice. HealthKit has given users more granular control over which data can be accessed according to which application is involved; in addition, in accordance with the relevant authorisation, HealthKit specifies who can access and see the data.

The actors involved in solving these threats are app developers, users, government, security professionals, and middleware vendors.

By the enforcement of the law, the market of mHealth can be regulated and contribute to technology. Certified mHealth applications need to comply with certain regulations by law.

4.2 Interviews

In this section, the results of the seven interviews, carried out to elicit vital information from relevant experts, are presented. The interviewees were from the medical health and security fields. Because anonymity was guaranteed, the interviewees' names are left out and have been replaced with 'XXX'.

Interviews were conducted with the following experts:

Table 10: Interview overview

Interviewee	Name	Occupation
a)	XXX	Philosopher and PhD student in mHealth
b)	XXX	Chief Security Officer
c)	XXX	General Practitioner
d)	XXX	Professional Welfare and Care Expert
e)	XXX	Professor

Additional interviews were held with non-experts in the field of mHealth applications. A fitness professional was interviewed because he also deals with clients that provide medical information so that a training schedule (for example, to lose weight) can be created. Therefore, the interviews elicited the provision of personal sensitive information. An important aspect of the fitness professional was that the information he provided protected confidentiality in handling. A supermarket manager was interviewed because he is using mHealth applications. Therefore, information from the users' perspective was also obtained.

Other interviews were undertaken with the participants listed below:

Interviewee	Name	Occupation
f)	XXX	Fitness professional
g)	XXX	Supermarket manager (mHealth user)

See Appendix A for a summary of the interviews.

4.2.1 Interview results

The benefits and threats related to mHealth apps that emerged from the interviews were scaled in accordance to how many interviewees gave the same answers. This enabled an analysis to take place

as to what the main benefits and concerns were in relation to accessing and storing personal EHR on mobile devices.

During the interviews, there was a slight distinction made between those who had experience about the topic of mHealth applications and those that were not familiar with the issue of eHealth and security. Those who were more concerned with their own different fields of expertise were more willing to take risks. The interviews related that there was a consistency of awareness across all interviewees that there were risks associated with the sharing of data. Interviewee a), for example, having studied the mHealth industry, was more concerned with the data breaches that are associated with mHealth apps. Interviewee b), the Chief Security Officer, had not looked into the rise in mHealth app usage, but did acknowledge the fact that personal data stored anywhere could be used by unwanted third parties; she was also aware that data that could be used to identify a single individual and associate him or her with private data that should not have been there in the first place. Interviewee c), the General Practitioner, was able to state that she thought that there were more benefits than risks to eHealth data; one of the risks she mentioned was that the use of mobile apps reduced personal social contact. Due to a case of personal blackmail involving someone she knew personally, she was, however, more cautious than she might otherwise have been. Interviewee g), the supermarket manager, did at one point mention that he did not felt anything was really missing in the security of his private data, but admitted he was not aware of how the data was stored or interfaced.

Those who were most knowledgeable and advanced in terms of eHealth apps agreed with the findings of other studies that more stringent guidelines and legal practices needed to be developed (Lusignan & Mold, 2016)

The results

Based on the interview results the benefits of and the problems associated with the use of eHealth apps are presented below.

The benefits are:

- ease of use (57 % gave this answer);
- efficiency and quality of healthcare (57 % gave this answer);
- remote control of and monitoring availability of service (43 % gave this answer);
- ease in accessing information and sharing it with more health professionals (43 % gave this answer);

- awareness of what an individual was doing and its impact on his or her health (29 % gave this answer);
- reduction in costs (14 % gave this answer); and
- reduction in hospital visits and an increase in the number of patients that could be helped (14 % gave this answer).

The potential threats are:

- Concerns were expressed about the privacy of data that is not well secured, and that other parties could access personal data (100% gave this answer).
- Uncertainty as to the reliability and validity of the information provided by mHealth apps (29%) gave this answer).
- Doubts were expressed as to how easily accessible the information was (14 % gave this answer).
- Concerns were expressed about the lack of regulation in the mHealth application market (14% gave this answer).

Safety of storage of Personal data

In the interview with experts in the field of health and security, the question asked was, 'Is it safe to transport and store personal medical data on mobile devices'? The following answers and assertions emerged as a result of this data:

1. 57% of the interviewees said that it was not safe to store and access personal health data on mobile devices.

The reasons that were given were:

- Third parties would be able to access personal health data.
- Not all mHealth applications encrypt personal identifiable data that is sent, meaning that other parties could see the data that was sent.
- mHealth applications and the data in it could be easily hacked.

2. 43 % of the interviewees stated that eHealth apps could be safe, but that this could not be guaranteed. These factors depended on:

- the user being able to secure his or her mobile phone with, for example, a pin code;
- whether a lot of information was shared with third parties without the knowledge of the users. Users often click on buttons without knowing what kind of access they are giving to third parties; and
- the right measures were in place to protect the information transmitted from the sender to the recipient.

3. 29% of the interviewees said that it is safe to access and send information to health professionals on via mobile devices.

- If the data is shared with the GP and s/he advises you do so (sharing with others in the medical field), then they thought it was safe because a person needed to trust his/her GP.
- Although they had had the experience that the sharing of information might not always be safe, they thought it should be done.

Furthermore, when answering the question: 'What is seen as the danger in privacy and security if patients independently create their own personal health records on mobile devices'? The following answers emerged:

1. 14 % of the interviewees stated that there were no dangers in patients independently creating and accessing their own personal health records on mobile devices. The reason was that users could control any dangerous aspects related to managing their own data.

2. 86% of the interviewees said that there were dangers in relation to the privacy and security of patients independently creating their own personal health records on mobile devices. The reasons behind these statements were as follows:

- A lot of information is shared with other parties without the users being aware that the information is being shared. The users could make that information secure by using codes or other authentication methods, such as biometrics.
- It was easy to link certain data to a particular person: If users were not aware of how to fill information in the mHealth applications, mistakes could be made and information might not be reliable and could even cause more harm than good.
- It was difficult for users to know what to save and how to navigate through the app.

Obtaining private data

In the interviews, the question that was asked was: 'How should private data be obtained'?

The results that came out of this question were:

- People need to be aware of what they are giving their permission for; the responsibility lies with each individual.
- All data that is retrieved, stored, or transported through mHealth apps should be encrypted.
- If servers are not guaranteed as being secure, that information should not be shared.
- The functionality should exist whereby the user can lock or delete data by remote control, if necessary.

- The user should be able to self-secure his or her mobile devices by locks on the device itself.
- Perhaps it is better not to create and store some data because 100% confidentiality can never be guaranteed.

4.2.2 Analysis

The main benefits and potential threats of eHealth apps with the outcome of interview results of chapter 4.2.1 are confirmed by the answers given by multiple experts.

To *solve* the potential threats the following solutions are provided:

- that all data that is retrieved, saved, and transported was encrypted;
- that information would not be shared with other parties;
- that users were schooled in knowing what they were giving permission to (and did not simply click on the permission button);
- that users understood how they could increase the security level of personal sensitive health data to make sure that their mobile devices themselves were secured by adding security mechanisms such as pin codes or the fingerprint functionality; and
- that functionality was created whereby users could lock or delete data by remote means.

The actors involved in solving these threats are the app developers and the users. It is clear from the research that the secure storage, transfer, and access of personal health data on mobile devices using mHealth apps is a concern shared by users. There is a feeling of distrust and uncertainty. To tackle this, awareness of the issues involved should be improved and checks should be put in place that informs users what information is being stored, how it is being stored, and what could happen to that data. Even companies operating under the strictest policies imposed either by the government or self-imposed, are still not impervious to hacks and leakages. This should be made completely clear to users before they access and use the facility. Third-parties have a special interest in mHealth app metadata and have developed sophisticated means to obtain it.

At least three interviewees mentioned that the high-profile data leaks that have led to, amongst others, Julian Assange's Wikileaks have given them the awareness that every person worldwide can be monitored and that every system is vulnerable to access by third-parties. Nothing is 100% safe. Government agencies worldwide might be able to access certain information, such as personal medical health records, although their aim might not be to steal this personal sensitive information. It is reported that the recent wave of attacks on medical institutions was executed using software created by the NSA which had been leaked and had been uploaded to Wikileaks and customised to suit the financial motives of the criminals (NPR, 2017).

4.3 The survey

In total, 50 surveys were conducted in the form of a questionnaire. The survey was divided into 3 age categories: 18 to 30, 30 to 50, and 50+. Every age category was divided equally into 10 males and 10 females, with exception of the 50+, which was comprised of 5 males and 5 females (see Appendix B for the survey questions and results).

4.3.1 Survey results

Usage of mHealth applications

78% of the respondents reported that they did not use mHealth applications because they were not aware of them, did not have an interest in using them or becoming familiar with these apps because they preferred face-to-face contact. This was also corroborated by the findings of the 2016 BMJ open study, which found that online access and services had an inconsistent effect on the frequency of face-to-face consultations, with some studies reporting a decline, some reporting an increase, and some reporting little or no change (Lusignan & Mold, 2016).

22% of the respondents indicated that they used mHealth applications. The type of mHealth applications that they used is summarised in Figure 7. The graph shows that the majority of the respondents either used an IOS or Android operating system.

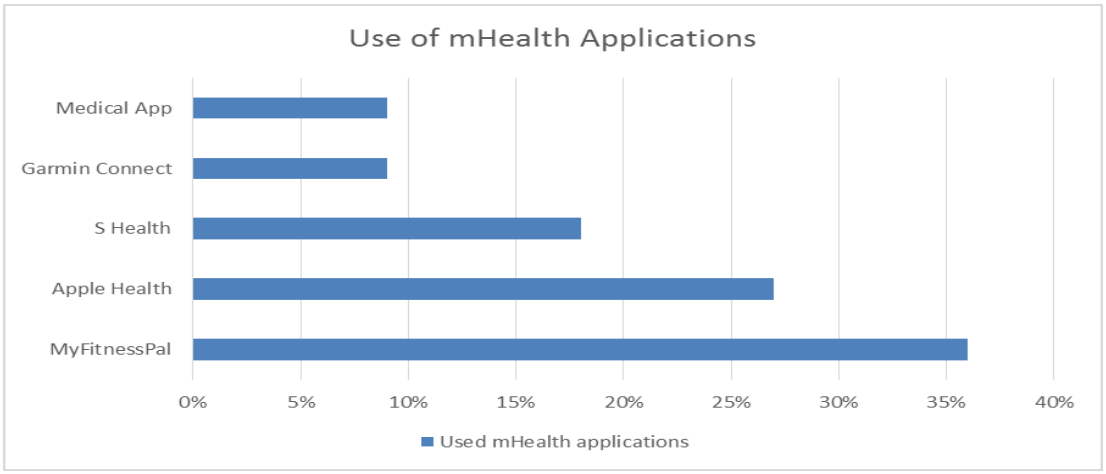


Figure 7: Percentages indicating us of mHealth applications

Figure 8 depicts the percentage of respondents that use these apps and which operating system they prefer to use when accessing mHealth applications. 10% of the respondents would not use any operating system for mHealth apps. This supports the usage already described in Figure 7.

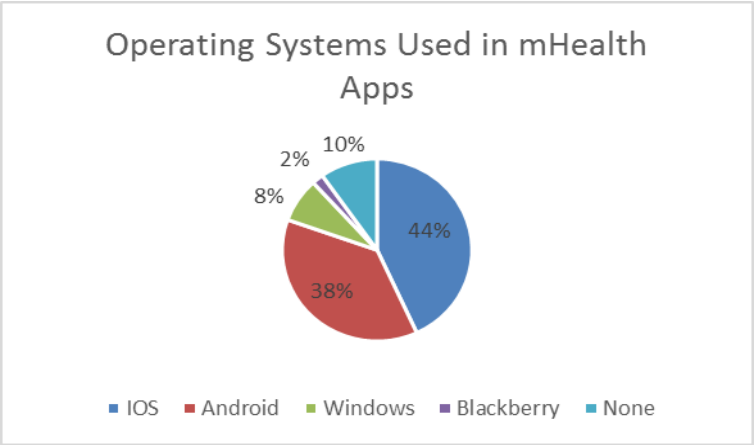


Figure 8: Circle Diagram mHealth OS

In terms of what the respondents thought in regard to the usage of mHealth application, the outcomes were:

26% were positive, because the respondents thought that these apps could improve people's healthcare and could provide information about the users' health; they thought that these apps would enable users to monitor their own health.

70% were neutral, because respondents were not familiar with mHealth applications; they did not see any personal benefits to using them.

4% replied in the negative, because they did not think that the apps added any value to their lives or that the use of mHealth applications is necessary for them.

Safety of mHealth applications

66% of the respondents did not think it was safe for their personal health data to be accessed and stored on mobile devices. The reasons behind this view were that:

- Other parties could access medical data and use it (since it was shared with other parties).
- Mobile devices were vulnerable and easy to hack.
- Privacy could not always be guaranteed.
- Terms and conditions often allowed for very unethical uses of the data.
- Users could not monitor who had access to his or her data.
- Users were not sure if the guarantees of confidentiality were matched in real life.
- Users were hesitant about having to depend on developers to do the right thing in terms of ensuring confidentiality.
- People were concerned about the number of data leaks.

34% of respondents thought that it was safe for personal health data to be accessed and stored on mobile devices, because:

- Such data could improve healthcare.
- Users or non-users were generally healthy (they thought) so there was no sensitive personal information to hack.
- They were not aware of any potential dangers.

Willingness to share personal data

Figure 9 summarises the percentage of which groups were willing to share personal health data.

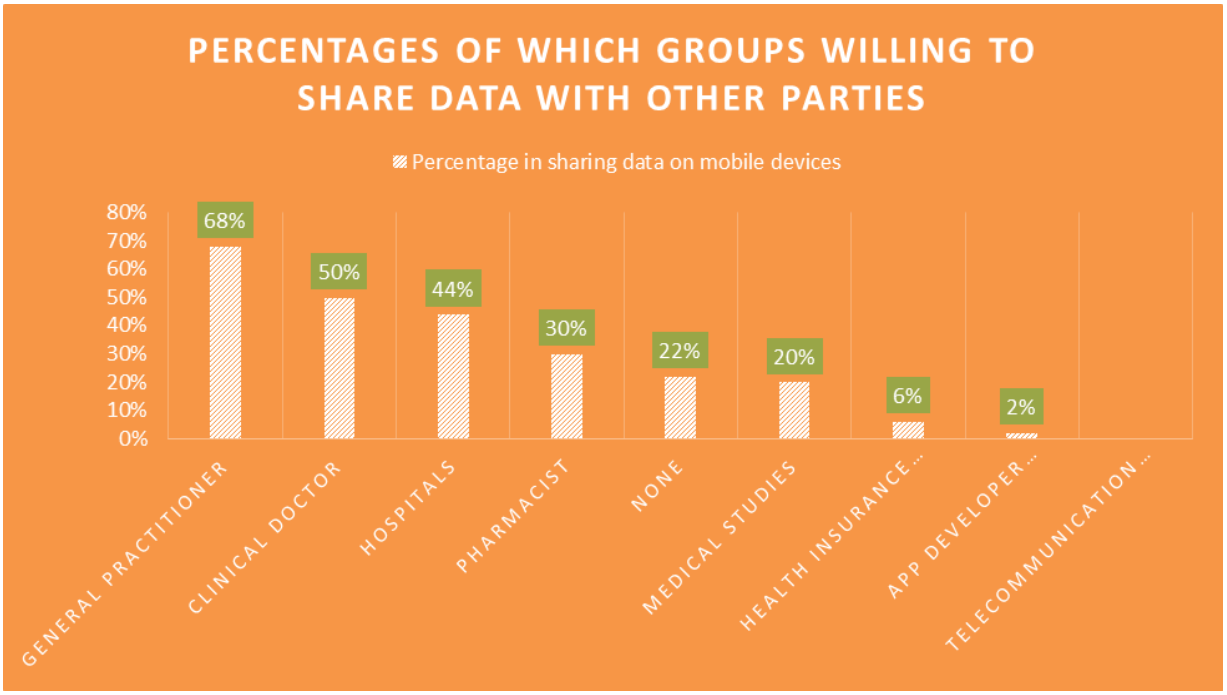


Figure 9: Chart showing percentages of which groups willing to share data with other parties

22% of the respondents in Figure 9 were not willing to share information with any other health professional or organisations through mHealth apps because they wanted their privacy maintained and believed that other parties might gain access to their personal health data, thereby compromising their privacy. See Appendix B for the survey questions and results.

4.3.2 Analysis

What emerged from the survey was that the main benefits of mHealth applications was they improved people's healthcare and provided information about users' health to relevant experts and groups. 78% of the respondents do not use mHealth applications. Thus 70% of the respondents were neutral about the usage of mHealth applications; this was a result of the fact that most of this group had no experience in using these apps and thus could not provide a review.

In terms of the threats involved in using these apps, 66% said they were not safe because

- Other parties could access people's medical data without them knowing the purpose for which it would be used.
- Terms and conditions often allowed for very unethical uses of the data.
- Mobile devices were very easy to hack and were, therefore, vulnerable.
- mHealth apps tended to reflect the interests of the developers (commercial considerations) and not of the users.
- Data was often and easily leaked.

Based on assessing who was most willing to share information via mobile devices with other health professionals, GPs demonstrated the most trust out of all the respondents. The 22% of this group who were not willing to share private data with other health professionals reflected the fact that the safety of information would not always be guaranteed.

Some of the solutions to potential threats that were suggested were:

- Users needed to be informed about the security of mHealth applications and needed to be assured that no one could access their personal information without them knowing that the information was being shared.
- Measures needed to be put in place to prevent other parties from accessing their personal health information.
- Clear and fair privacy policies for users needed to be drafted.

The principal groups involved in these issues are the users and app developers, and it is very important that regulations and controls are drafted.

4.4 Correlations

Literature review vs interviews

A review of the relevant literature corroborated the findings of the interviews. Thus, the benefits and the potential threats of the use of eHealth apps are similar, see Chapter 4.1.5(analysis literature review) and 4.2.2 (analysis interview results). The interviews revealed that the perceived risks were outweighed by the practicality of having mHealth apps, a finding similar to one study which expressed the end-users' willingness to trade-off security for ease of access (Lusignan & Mold, 2016)

The similarities back this study's findings that the data is not well secured and that it is easy for sensitive information to be hacked. Both users and app developers have a measure of responsibility in terms of the issues of privacy and confidentiality. Users should check to see what they are clicking on and who they are granting permission to in terms of accessing their information, and developers

need to ensure that they are abiding by guidelines and implementing relevant security mechanisms. If both sides do their part, the privacy and security of information on mHealth applications on mobile devices can be assured.

It can be confirmed that the threats perceived by the interviewees are in line with the experiences and research that have already been presented; in short, all the information gathered confirms their perception that they are not totally secure in terms of their information. There are methods that can secure personal medical data, but many of those methods are not being applied. General security measures need to be taken to solve the gaps in the privacy and security on mobile devices. In Chapter 5.3, recommendations will be given to clarify which measures should be drafted and applied.

Interviews vs survey → Literature

The gaps in the privacy and security in relation to personal EHR on mobile devices are issues that are acknowledged in survey results, literature reviews, and interviews. However, in the survey conducted during this research, 70% of the respondents held a neutral view, but that finding was a result of the fact that they did not have hands-on experience with mHealth applications and were not familiar with how this software worked. Because they were not familiar with eHealth apps, they were not aware of any personal benefits to their use and thus also were ignorant of the potential threats. 66% of the respondents stated that the access of personal EHR on mobile was not safe because third parties could access users' medical data without their knowing why it was being accessed.

The findings of the interviewees who have studied or work with mHealth apps correlated to the findings in studies reflected in the relevant literature, such as the analysis conducted by BMJ Open in 2016, which demonstrated that patient connectivity and the services offered by mHealth technology enhanced convenience in terms of the health professionals and improved the users' sense of satisfaction.

5 Discussion

This study reflects the results of an analysis that was undertaken as to how the privacy and security of personal EHR records stored and accessed on mobile devices could be ensured; it was undertaken so that recommendations could be made both to users and to app developers as to how confidentiality could be protected and incidents of hacking and leaking minimised. This chapter reveals the findings of the investigation and discusses the potential threats that exist in relation to the actors that are involved in the security of mHealth applications.

The discussion begins with a description of the actors concerned and what their roles and responsibilities are in keeping personal sensitive information on health records safe. In addition, recommendations as to the guidelines that need to be drafted and the security frameworks that need to be created will be made so that mHealth applications meet the required standards of security, privacy, and confidentiality.

5.1 Actors in mHealth applications

There are a number of key actors that are involved in app security, and each actor has his or her role to play in sustaining and contributing to a safer environment for accessing and storing personal electronic data on mobile devices. The risks involved and how to address them should be made clear after this chapter. The potential threats mentioned in Chapter 4 will be associated with actors that have a direct impact on eHealth app security and privacy; as discussed previously, the principle two groups involve users and app developers. In terms of receiving information and ensuring that the data received is kept safe, medical professionals also have a role to play. Additional actors will also be added to the groups and individuals that are being discussed, since they also participate in regulating and maintaining the privacy and security of personal EHR on mobile devices. The principal groups of actors discussed are:

- users (of mHealth applications);
- app developers;
- professionals from the medical and security fields;
- regulators (government personnel, auditors, and certified agencies); and
- vendors (of medical devices and hardware).

Role and responsibilities: The users make daily use of mHealth applications; they need to check which mHealth applications they give permission to and what they are downloading.

Relationship to other actors:

App developers: The app developer is the supplier of the mHealth applications that users utilise.

Medical professionals: The medical professional receives the information that the user sends. The receiver of the data needs to handle it in a confidential manner. Although the issue is that commercial parties like Apple, Google, Fitbit also receive the information the user sends. Whereby they might not handle personal sensitive data in a confidential manner. These commercial parties could use the information for unintended purposes without the knowledge of the user.

Government: The government needs to inform users about their rights concerning the misuse of personal sensitive data.

Hardware vendors: This group supplies the hardware (mobile devices) that users utilise to download or access mHealth applications. They provide the basic built-in security of hardware.

Share in the risks: The users are the owners of the personal sensitive health data. Their share in the risks involved is that, if they are unaware of potential threats, they might give permission to other applications to access their mobile devices without verifying if the application is safe. In addition, they bear the responsibility of ensuring that their mobile devices are secure. They need to educate themselves as how to properly use eHealth applications.

Measures to be taken to eliminate risks: The users need to educate themselves in relation to how to maintain mobile device safety and security and what questions they need to ask before they grant permission for their device to be accessed. This can be achieved by them reading privacy policies, by maintaining self-security on the mobile device, and by checking if the mHealth application is certified. A certified application spells out clear conditions and terms apply to a particular mHealth application. Self-discipline and self-awareness are key traits that users should develop.

Role and responsibilities: App developers are the suppliers (providers) of mHealth applications and, in light of this fact, they need to ensure that privacy and data are protected. App developers are responsible for making sure that end-users are made fully aware of how data will be used by the app and by their company.

Relationship to other actors:

Users: Users are the consumers that purchase mHealth applications.

Medical professionals: Because this group receives the data that is sent via mHealth applications, they need to involve medical professionals during the process of app development.

Security professionals: This group needs to be involved in advising app developers in how to secure all the aspects that need to be considered in order to prevent any gaps in the security and privacy of mHealth applications (e.g. through ethical hacking).

Government: Legislators of the laws and regulations concerning privacy and security of personal sensitive data and they do the drafting. App developers need to be aware of governmental and other regulations when they are developing their applications.

Certified agency bodies: They assess mHealth applications to ascertain if the apps conform to legal requirements and to technical standards.

Medical hardware vendors: Medical hardware vendors in making sure that the device connected with the mHealth application is secured. The mHealth applications will be accessed or stored on the mobile device (hardware). The communication of the medical devices and mobile devices needs to go via secured connection.

Middleware vendors: They provide middleware for app developers so they do not have to write the whole code for mHealth applications but only a piece. These middleware vendors like Apple HealthKit have already implemented security measures that app developers can use in creating the application.

Share in the risks: App developers share their risks if they do not secure the applications in terms of:

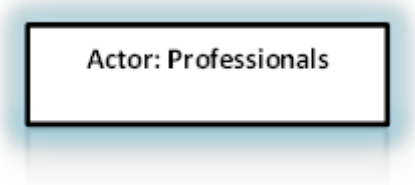
- data stored and transmitted in their mHealth application is not encrypted;
- lack of clarity in terms of where the data is stored;
- poor authentication and authorisation;
- data shared with other parties;

- uncertainty, reliability, and validity of information provided by mHealth apps;
- privacy policies not created according to the HIPAA or EU Data Protection Law;
- making user interfaces the main priority for commercial purposes whereby the security of applications does not get the attention it should get.

The app developer shares a lot of risks in the retrieval, storage, and transmission of personal sensitive data.

Measures to be taken to eliminate risks: the app developer needs to do the following:

- Apply security measures in the design of mHealth application such as when designing the user interface.
- Apply encryption in the storage and transmission of personal health data.
- Apply two-factor authentication and authorisation controls.
- Avoid sharing data with other parties without taking the concerns of users into account.
- Create awareness of the importance of applying privacy policies that conform to HIPAA regulations.
- Apply API frameworks like Apple HealthKit, which will give the user more granular control over their data.



Medical professionals

Role and responsibilities: Healthcare professionals must follow the given security procedures in terms of the privacy and confidentiality of the data they receive from the users (patients or consumers) of mHealth applications. They have an ethical duty towards their users (patients).

Cooperation with other actors:

Users: Medical professionals receive personal sensitive information from the users and there is an exchange of information between these two groups.

App developer: App developers need to involve medical professionals while they are in the process of developing eHealth apps, since the medical experts receive the information sent by the mobile app.

Government: They draft the laws that should ensure the privacy and confidentiality of users.

Hardware vendor: Supplier of the mobile device in receiving personal health data.

Share in the risks: Any threat to patient health-related data is a threat to doctor-patient confidentiality. Doctors are bound by the 'Hippocratic Oath', and thus must do everything possible to ensure patient confidentiality. A doctor who does not follow the guidelines and proper procedures

and who encourages the installation of unwarranted malicious apps for day-to-day tasks has inadvertently put a patient's data at risk. The professionalism of the doctor will come into question if it is found that technological negligence has led to a data security breach.

Measures to be taken to eliminate risks: Healthcare professionals must be up-to-date and informed about data security safeguards, what a professional can and cannot do with hardware and software. They should not encourage the use of apps and hardware that have not been approved as being safe and legitimate.

Security Professionals

Role and responsibilities: Security professionals must continuously monitor and improve data security and must ensure that the best possible security policies are being implemented at all times. Those responsible for security must make sure that access to systems and data is highly selective and based on proof of necessity (role). They must, all times, apply the CIA principle: confidentiality (=encryption, selective and explicit authorisation); integrity (consistency, accuracy, maintaining the trustworthiness of the data over its lifecycle); availability (keeping security measures up-to-date by patching, making use of operating system updates to block attacks, updating and maintaining security frameworks (such as HealthKit) in general and specifically.

Relationship with other actors: These experts are responsible for implementing proper and adequate data-security. They have to be aware of what precautions the app developers are using when the software is being created and of how the data will be interfaced. They will inevitably have to take into consideration the existing legal frameworks (governmental guidelines and regulations) and what possibilities and risks are associated with which hardware.

Share in the risks: Security officers have a broad range of responsibilities, all focused on one target: ensuring security. Hence, the success of any third-party in accessing and misusing personal data is a direct infringement on the role of the security officers in charge. Security officers will then be pressured by healthcare agencies, governments, and the end-users to determine whether there was a lapse in security and whether or not the overarching framework needs improvement.

Measures to be taken to eliminate risks: Those whose task it is to ensure security do so by implementing the best practices and hardware/software/networking configurations to facilitate the secure transfer of data. They are in charge of making sure the technical, administrative, and physical safeguards are all in place. Applying ethical hacking to ensure that the mHealth applications are safe from any intrusion in authority from the app developer.

Government

Role and responsibilities: Regulators are responsible for the contribution of drafting laws that will support technologies that will ensure that the privacy and security of citizens using eHealth apps is guaranteed.

Relation with other actors:

Users: Governments are tasked with protecting their citizens through national and international policy-making. When security measures fail and calamities happen, governments are left with the task of restoring the situation by coming up with solutions for the societal sectors affected; they are also responsible for reporting accurately and transparently on the severity of the catastrophe to the public. As was seen during the WannaCry scare of May 2017, governments become highly engaged with their economic sectors and other governments during national and cross-border cyber-attacks.

Share in risks: Governments are directly and indirectly affected by disruptions and outages that affect people and businesses. The infiltration of health-related data by an unwanted party compels governments to act whether they are directly affected or not. Citizens and businesses that have had their data misused will inevitably look to the government for solutions and for the creation and application of new policy guidelines. Healthcare providers, such as the NHS, which are publicly run entities, have direct links with the government, meaning that government systems can become compromised.

Measures to be taken to eliminate risks: Governments collaborate with certified public and private entities to come up with solutions and binding legal frameworks that cover personal healthcare data and protect consumers from harm. They can increase the budget allocated to cyber-security and implement their own security strategies and technologies.

Certified agencies (in this case our suggested PriSecure Certification)

Role and responsibilities: These agencies are tasked with making sure that mHealth applications are certified according to officially defined frameworks and regulations governing every aspect of security by design and default. Meaning that security has already been applied during the design phase of the mHealth application.

Relationship with other actors:

Auditor: The auditor is responsible for supervising the agency to ensure that quality is being delivered and it is fulfilling its requirements.
App developer: The certified agency body provides the app developers with a quality mark (certification) when they apply for it.
Users: users can check if a mHealth app carries the appropriate certifications, ensuring that independent third parties has audited the app against the necessary requirements of the certificate.
Share in the risks: A risk is if they certify mHealth applications that do not meet the requirements of receiving a quality mark users will lose confidence in the safety of these applications.
Measures to be taken to eliminate risks: Certified agencies need to make sure that all certified apps meet the requirements for the provision of a quality mark.

Auditor

Role and responsibilities: Examines and double checks certified apps. In making sure that there is an assurance in the quality of mHealth applications.
Relationship with other actors: Auditors check the accuracy and trustworthiness of the certification process and report back to the certified agencies. This can be to the government or other parties like for example NIST.

Share in the risks: In double checking the certifications of mHealth apps to prevent leakage of data.
Measures to be taken to eliminate risks: Auditors must verify that security measures are being correctly and rigorously applied, impose punishments on app developers and/or certified agencies if security measures have not been put into place.

Medical hardware vendors

Role and responsibilities: Vendors must ensure that medical devices meet the standards and requirements of existing legal frameworks. They are also responsible for developing new ways to protect the devices from unwarranted access.
Relationship with other actors:
Users: Vendors provide the hardware and devices to the users.

Share in the risks: Hardware developers are keen to implement whatever mechanisms they have at their disposal to deflect, in a timely fashion, cyber-attacks being carried out on mobile devices, that is, before the hackers have had the chance to access private data.

Measures to be taken to eliminate risks: Hardware vendors need to develop technological safeguards that make their hardware safer; in addition, the need to draft and provide extensive documentation on how users can best protect data when using their devices.

5.2 Summary of threats and ways to reduce risk in mHealth security

The table below summarises the threats to the security of mHealth apps and suggests what measures need to be taken to secure personal electronic health records on mobile devices

Table 11: Threats and ways to reduce risk in mHealth security

Category	Threats	Solution	Actor responsible
Legal	Lack of regulation of the mHealth app market	Making sure that there are standards to certify applications that can regulate the quality of mHealth apps	(1) Security Professional (2) Certified agency body *('PriSecure certification')*
	Privacy policies are not properly drafted and are not and clear to users	Privacy policies should conform to the HIPAA or to EU data protection law	App developers
Educational	Lack of knowledge on the part of users	Educating users about how to enhance the security of these apps	(1) App developers (2) Medical professionals (3) Users
	No clarity about where data is stored	Providing a machine readable format with information about what is stored and where	App developer
	Users give permission without	Checking the standard of regulations of the	User

Usability	knowing what they are agreeing to	application and checking the quality marks of mHealth applications	
	mHealth app made for commercial purpose in gaining profit instead of focus on privacy and security	Security and privacy should be observed and applied in mHealth applications that are being built	(1) App developers (2) Security professionals
Technical	Data is stored, retrieved and transmitted without encryption	All data stored, retrieved, and transmitted needs to be encrypted	App developers
	Poor authentication and authorisation controls	Applying two-factor authentication and strong authorisation controls (giving users more granular control); using an API framework like HealthKit	
	Personal sensitive information shared with third parties	Not sharing information with third parties not using their service	
	Uncertainty about the reliability and validity of the information provided by mHealth apps		
	Conceptual weaknesses in the operating system	Checks are done by hardware vendor	Hardware vendor

5.3 Recommendations

Identifying potential threats, observing existing guidelines and laws that already exist (and drafting new ones, if required), and implementing the recommendations and have been made will minimise the risks associated with mHealth data storage. To regulate the market of mHealth applications and ensure the privacy and security of users, the first step that should be taken involves the certification of mHealth applications.

Certification process

The certification process of mHealth applications should be amended in the following way:

1. Governments need to take responsibility for accreditation or making sure that other institutions outside the government take that responsibility to assure the safeness in the eHealth industry.
2. Certain certified agencies should be given a licence, which will enable them to check the privacy and security of mHealth applications.
3. A document containing standard guidelines should be drafted by a standards creating institution with specific knowledge on security requirements in the healthcare and eHealth.
4. App developers or other creators of mHealth apps need to be told the conditions of certification and need to know what requirements they need to meet *('Prisecure certification').*
5. When the mHealth app is assessed, and the app passes, a quality mark *('PriSecure certification')* needs to be issued.

The steps for applying for 'PriSecure certification' are as follows:

1. The mHealth developer applies for a security assessment that will prove that physical, technological, and social safeguards are in place.
2. The agency bodies grant the request and carry out a security assessment requiring that the following are in place in table 12:

Table 12: Requirements for secure mHealth apps

The requirements	Clarification of requirement
Access control and authentication	Does the user have the ability to disable this access at will? What kind of unique ID is used? How is it accessed? (Martinez-Perez, del Torre-Diez,

	Lopez-Coronado, 2015)
Security and confidentiality	What is the encryption level? What is the ability to be breached by cybercrime?
Informing users	The end-user agreement, privacy policy – outlining the risks to the end-user. Users need to be informed before privacy policies changes and terms used in these policies needs to be explained proper and no vague terms
Data transfer	The medium through which data is transferred, is user aware what is being transferred when?
Data retention	For how long (if at all) does this information remain within the app and the receiving device and is this featured in the end-user agreement?
Breach notifications and legal obligations	How (and to what level) are patients or health institutions informed in the event of breaches and what controls to take in such an event? i.e. If breaches affect a significant number of users, will the media be notified? (Martinez-Perez, del Torre-Diez, Lopez-Coronado, 2015)
Delete function users	There need to be a functionality where the consumer can delete all data from the providers when needed.
Machine readable format users of personal data	The providers needs to provide a machine readable document for the user. So that the user can see which information the provider has and for which reason it is processed.
Details of app developer needs to be provided	The providers should let their contact details and address be visible for the users of mHealth applications.
Users granular control	Users need to get granular control over their personal data and can decide whom can see

which data.

3. The applicant can be rejected then it needs reassess its application and if it is accepted the mHealth application gets a logo of “PriSecure certified”.

Operating system requirements

It has been reported that 90% of the NHS computers were exposed to the recent WannaCry infection because they were still running on Windows XP (Kennedy, 2017). In the case of mobile devices, the operating systems of Android and IOS need to inform the users in their stores of the dangers of mHealth applications and explain what “PriSecure certification” is. They also need to remind users how they can protect their devices when they use apps downloaded from mHealth area within the Apple or Google Play Store. Users need to be educated about good security procedures and need to be made aware of the dangers.

Users

In terms of the users, they are responsible for checking if the mHealth application is certified before downloading any application and entering their personal information. They need to read the instructions and warnings and not simply ‘click’ automatically, thus granting permission before they know what they are agreeing to.

Final remarks

Upcoming APIs also need to be certified to ensure that, when mHealth applications use those APIs, security concerns are addressed.

As the health industry moves into new directions, HIPAA regulations and EU data protection laws can support the enforcement of security procedures guaranteeing privacy and confidentiality. The technologies that will be mentioned in section 6.1.3 will contribute to greater privacy and secure environment for mHealth apps.

6 Conclusion

6.1 Conclusion

6.1.1 RQ1 What are the benefits and threats of using EHR on mobile devices?

The research reported in this paper has clarified the benefits and the potential threats of using and storing EHR on mobile devices. The conclusion has been reached that the crucial advantage of accessing personal EHR on mobile devices is ease of use: in other words, people can use, access, and update personal medical information at any time and the app can even run autonomously. Patients can also use their mobile devices to access, record, and send their medical status to relevant professionals and can communicate with the device remotely. The result is that health professionals free up some of their time as visits to GPs become less frequent. This will improve the availability, effectiveness, and affordability of healthcare. Both patients and medical professionals benefit as users of mHealth apps become more aware of their medical status.

The main threat that arises from the use of eHealth apps on mobile devices is the right to privacy and security cannot be guaranteed. The primary causes of these threats is that authorisation and authentication procedures are poor, data storage is insecure, data is not properly encrypted (either when it is sent or received), users are not aware of the permissions they are granting, and the market is poorly regulated. It is clear that proper, rigorous guidelines need to be created to tackle this issue. In this context, see Chapter 4.1.5 (analysis of the literature), Chapter 4.2.2 (analysis on the interviews), and Chapter 5.1 (mHealth actors involved in the process of security) for a detailed discussion of these points.

6.1.2 RQ2 How secure are the current available apps and APIs (application programming interfaces) on the market that handle EHR data on mobile devices?

The current available applications handling EHR data on mobile devices are not all sufficiently secure. This means that outsiders might potentially have access to personal EHR in these vulnerable apps stored on mobile devices; in other words, people's information can be hacked, exploited, and sold if current applications do not all use up-to-date security technologies (although APIs do apply some sort of technology that is meant to protect personal sensitive information). APIs like the Apple HealthKit can assure the safety of personal health information. An example of an application that applies this API is Apple Health. The up-to-date security technologies are described in section 6.1.3. Section 4.1.2 also provides additional information. The lack of encryption contributes to the vulnerability of the information.

6.1.3 RQ3 Are there existing technologies that can improve data security and the storage on mobile devices?

The existing technologies that can improve data are: two-factor authentication, authorisation control, encryption technology, data breach notifications, and server control security. Furthermore, if mHealh applications use APIs (such as HealthKit), the HIPAA and EU data protection law and a security assessment covering technical, physical and administrative safeguards that are earlier described in section 2.2.1. security will also be enhanced. This all is supported in section 4.1.3, 4.1.4, and Chapter 5.

6.1.4 RQ4 What specific additional mechanisms are needed on top of default security measures in mobile devices that contain and handle EHR data to improve medical confidentiality?

To improve the medical confidentiality of EHR on mobile devices, the technologies mentioned in section 6.1.3 need to be applied. For example, the use of two-factor authentication is necessary in order to ensure that the right person is accessing the medical data.

Furthermore, all privacy and security dimensions in the taxonomy need to be covered by the security assessment (described in 4.1.3; the recommendations are found in section 5.3). In addition, it is crucial that users are educated about how they themselves can also contribute to securing their data, for example by adding extra security measures to their mobile devices. One critical step that should be undertaken is making mHealth apps secure by design and default. This in making sure that security mechanisms are already in place when designing the mHealth application and the purpose of the processed data needs to be clear and secured as stated in EU data protection law 'Article 25'.

6.1.5 What can be done to enhance the security and confidentiality of personal EHR data stored and handled on mobile devices whilst granting patients more granular control over their data?

The research undertaken leads to the conclusion that the factors listed below will enhance the security and confidentiality of personal EHR stored on mobile devices:

1. All personal data transferred through mobile devices need state-of-the-art, end-to-end **encryption.**
2. Users should be sufficiently **informed** about the threats to privacy and security of mHealth data by the App store or by developers.
3. The apps should **conform** to international or European Union laws on data security by design and default. Privacy policies conforming to the HIPAA and EU data protection laws need to be made clear.
4. The mHealth market should apply the requirements as mentioned in our *"PriSecure certification"* to **regulate** the market (described in section 5.2, 5.3).

5. Strong **authentication and authorisation controls** are needed. Like Apple's HealthKit API grants users the permission to control these security mechanisms.
6. The functionality of **patients granting** granular control over their personal sensitive data. The patient can decide which data item will be visible for which party. APIs like Apple HealthKit grants users to have granular control over their health data.

Finally, if all the recommendations in Chapter 5.3 are followed, the security and confidentiality of mHealth applications should be significantly enhanced.

6.2 Recommendation for future research

One issue that needs to be explored in future research is how to enhance the integration of personal EHR hosted on the servers of the hospitals with the need for patients being able to access this on mobile devices. This falls out of the scope of the research carried out in this study, and was, therefore, not investigated.

References

Adhikari, R., Richards, D., & Scott, K. (2014). Security and Privacy Issues related to Use of Mobile Health Apps. *Australian Conference on Information Systems (Auckland)*.

Aitken, M., & Gauntlett, C. (2013). *Patient apps for improved healthcare from novelty to mainstream.* Parsippany (NJ): Institute for Healthcare Informatics.

API Academy. (n.d.). API Strategy: What is an API?

Apple. (2013). *HealthKit documentation.* Retrieved 2017, from Apple Developer: https://developer.apple.com/healthkit/

Apple Inc. (2016). *HealthKit*. Retrieved from API Reference: https://developer.apple.com/reference/healthkit#//apple_ref/doc/uid/TP40014707

Brandom, R. (2017, May 12). UK hospitals hit with massive ransomware attack. *The Verge*, p. 1.

Cousin, Castilo-Hi, Snyder. (2015, 9 11). *Deloitte University Press: Devices and diseases: How the IoT is transforming medtech*. Retrieved from The Internet of Things in the medical devices industry: https://dupress.deloitte.com/dup-us-en/focus/internet-of-things/iot-in-medical-devices-industry.html

CSO. (2014, May 21). *Relentless cyber criminals are always looking for the next big hack, and mobile devices are the new frontier*. Retrieved from CSO online: http://www.csoonline.com/article/2157785/data-protection/five-new-threats-to-your-mobile-device-security.html

Cubrilovic, N. (2014). *Notes on the Celebrity Data Theft.* Nikcub.com.

Data Protection Commissioner. (n.d.). *Data Protection*. Retrieved from Anonymisation and pseudonimisation: https://www.dataprotection.ie/docs/Anonymisation-and-pseudonymisation/g/1594.htmv

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 or Android. *Security and Privacy of mHealth and eHealth*.

Ehrenfeld. (2017, May 24th). *WannaCry, Cybersecurity and Health Information Technology: A Time to Act.* Retrieved from Springer Link, Journal of Medical Systems: https://link.springer.com/article/10.1007%2Fs10916-017-0752-1

European Commission. (2014, September 2nd). *European Commission.* Retrieved from Remote monitoring with mHealth can reduce healthcare costs: https://ec.europa.eu/digital-single-market/en/news/remote-monitoring-mhealth-can-reduce-healthcare-costs

European Parliament and Council of European Union. (2016). *European General Data Protection Regulation document.* Brussels: European Union.

European Parliament and the Council of the European Union. (2016). *European General Data Protection Regulation.* Brussels: European Union.

Google. (2016, June 2nd). *Google Terms and Conditions*. Retrieved from Google Developers Guide: https://developers.google.com/fit/terms

Guardian. (2017, May 13). NHS seeks to recover from global cyber-attack as security concerns resurface. *The Guardian*.

Hedge, M. (2016, February 3). *Cloud Storage VS Local Storage- Which is Right for your business.* Retrieved from Contegix: https://www.contegix.com/cloud-storage-vs-local-storage-which-is-right-for-your-business/

HIMSS. (2017). *Dictionary of Health Information Technology Terms, Acronyms and Organizations.* Orlando: CRC Press.

Huckvale, K., Prieto, J. T., Tilney, M., Benghozi, P.-J., & Car, J. (2015). Unadressed privacy risks in accredited health and wellness apps: A cross-sectional systematic assessment. *BMC Medicine*.

IBM. (2016). *2016 Cyber Security Intelligence Index.* IBM.

Infosec. (2014). *Remote Access Tool.* InfoSec Institute.

Kennedy, R. (2017, May 17th). *Cyber Security Data Breach Affects the National Health Service.* Retrieved from Lexology: http://www.lexology.com/library/detail.aspx?g=90d18fb5-2b64-4aaa-977d-1027af833481

Kumar, Lee. (2012). Security Issues in Healthcare Applications Using Wireless Medical Sensor Networks: A Survey. *Sensors*, 55-91.

Lusignan, S. d., & Mold, F. (2016). *Patients' online access to their electronic health records and linked online services: a systematic interpretative review.* group.bmj.com.

Mark Saunders, P. L. (2009). *Research methods for business students 5th edition.* London: Pearson Education Limited.

MarketsandMarkets. (2014). *Mobile health apps & solutions market by connected devices (cardiac monitoring, diabetes management devices), health apps (exercise, weight loss, womens's health, sleep and meditation), medical apps (medical reference)- global trends & forecast to 2018.*

Martinez-Perez, del Torre-Diez, Lopez-Coronado. (2015). Privacy and Security in Mobile Health Apps: A Review and Recommendation. *Journal Medical Systems*.

Mense, A., Urbauer, P., Wahl, H., & Sauerman, S. (2016). *Analyzing privacy risks mHealth applications.* Wien- Austria: FH Technikum Wien, University of Applied Science.

NHS. (2015). Health Apps Library.

NPR. (2017, May 15th). WannaCry Ransomware: Microsoft Calls out NSA For 'Stockpiling Vulnerabilities. *NPR*.

Perez Morera. (2016). Security Recommendations for mHealth apps: Elobaration of a Developer's Guide. *Journal Medical Systems*, 1-13.

Planchkinova, M., Andrés, S., & Chatterjee, S. (2015). A Taxanomy of mHealth apps- Security and Privacy concerns. *48th Hawaii International Conference on System Sciences.* Claremont- USA: Claremont Graduate University.

Radet, F. (2016). *Appfail.* Norwegian Consumer Council.

Samsung. (2016, April 6th). *S Health and Samsung Digital Health SDK*. Retrieved from Mobile tech Insights Samsung Developers: http://developer.samsung.com/tech-insights/health/shealth-and-samsung-digital-health-sdk

Samsung Electronics Co. Ltd. (2016). *Samsung Knox Security Solution.* Samsung Research America.

Staimer, M. (2012, August). *Cloud backup versus cloud storage comparison.* Retrieved from SearchDataBackup: http://searchdatabackup.techtarget.com/tip/Cloud-backup-versus-cloud-storage-comparison

Tom, D. (2014, June 3). *The Data Management Debate: local vs. cloud storage.* Retrieved from Storage Craft: http://www.storagecraft.com/blog/the-data-management-debate-local-vs-cloud-storage/

U.S. Department of Health and Human Services. (2013, July 26). *Summary of the HIPAA Security Rule.* Retrieved 2013, from HIPAA: https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

U.S. Department of Health and Human Services. (2016). *Examining Oversight of the Privacy and Security of Health Data Collected by Entities Not regulated by HIPAA.* Washington.

U.S. Department of Health and Human Services. (2016). *Examining Oversight of the Privacy and Security of Health Data Collected by Entities: Not regulated by HIPAA.* Washington.

WHO. (2011). *mHealth New Horizons for health through mobile technologies.* Switzerland: World Health Organization and Global Observatory.

WHO. (2015). *eHealth at World Health Organization*. Retrieved from eHealth: http://www.who.int/ehealth/en/

World Medical Association. (2016). WMA Statement on Cyber-Attacks on Health and Other Critical Infrastructure. *67th World Medical Assembly.* Taipei- Taiwan: World Medical Association.

Xinfeng, Bakh. (2015). Fine-grained access control for cloud computing. *International Journal of Grid and Utility Computing*, 95-102.

Yang, B. (2016). *What Makes You Sure that Health Informatics is Secure.* Norway: Norwegian Information Security Laboratory (NISlab) and Center of Cyber and Information Security (CCIS).

Zhang, S. (2017). *Local storage vs Cloud storage: Which is better for your Personal Data Backups?* Retrieved from Datanumen: https://www.datanumen.com/blogs/local-storage-vs-cloud-storage-better-personal-data-backups/

Zubaydi, F., Saleh, A., Aloul, F., & Sagahyroon. (2016). *Security of Mobile Health (mHealth) Systems.* Sharjah, UAE: American University of Sharjah.

Glossary/ Acronyms

	Acronym	Full word	Definition
A	APP	Application	Application on a mobile device
	API	Application programming interface	Set of routines, protocols, and tools for building software, specifying how software components should interact
E	eHealth	Electronic health	The use of information and communication technologies (ICT) for health-related medical purposes
	EHR	Electronic health records	Digitalised records of someone's medical history
F	FTC	Federal Trade Commission	Set up in 1914, an agency that is independent of US government.
	[redacted]	Fully-fledged	Developed or matured to the fullest degree
H	HIPAA	Health Insurance Portability and Accountability Act	US legislation passed in 1996 and which governs the health sector
	HITECH Act	Health information technology for Economic and clinical health act	U.S. regulation passed in 2009 to support electronic health records
	[redacted]	Health plan entities	The health plan is the health, dental. Vision maintenance organisations. It includes sponsored employer group health plans
	[redacted]	Health care cleaning houses	The processing of non-standard information received from other entities in the standardisation of data
	[redacted]	Health care providers	They electronically provide transactions as submission, claims and prior authorisation (U.S. Department of Health and Human Services, 2016)
M	mHealth	Mobile health	'the practice of medicine and public health supported by mobile devices such as mobile phones, patient monitoring devices, personal digital assistants and other wireless devices' (WHO, 2011)

O	OWASP	Open Web Application Security Project	Is an organisation that helps in the development, maintenance and purchase of applications that are trustworthy
P	PHI	Personal health information	This refers to health data that is identifiable to the person involved
	[redacted]	Pseudonymisation	This term refers to replacing any identifying characteristics of data with a pseudonym, or, in other words, a value which does not allow the data subject to be directly identified (Data Protection Commissioner)
S	SDK	Software development kit	A set of tools to develop software in a certain package to create apps
W	WHO	World Health Organisation	International Health organisation of the United Nations specialises in maintaining global health

List of figures

List of tables and graphs

Appendix A: Interview

Mail for interviewee

Interview summaries

a) **Interview Summary mHealth apps- Philosopher and PhD student in mHealth**

b) **Interview Summary mHealth apps- Chief Security Officer**

c) **Interview Summary mHealth apps- General Practitioner**

d) **Interview Summary mHealth apps- Professional Welfare and Care Expert**

e) **Interview Summary mHealth apps- Professor**

f) **Interview Summary mHealth apps- Fitness professional**

g) **Interview Summary mHealth apps- Supermarket manager (mHealth user)**

Appendix B: Survey results

Survey Introductory Letter

Survey Questions

Survey Results

See attachment document for Appendix A and B