Health Informatics Journal

Regular Article

A review of privacy and usability issues in mobile health systems: Role of external factors

Health Informatics Journal
2019, Vol. 25(3) 935–950

DOI: 10.1177/1460458217733121
journals.sagepub.com/home/jhi
SAGE

Jane Katusiime
Humboldt-Universität zu Berlin, Germany; Mbarara University of Science and Technology, Uganda

Niels Pinkwart
Humboldt-Universität zu Berlin, Germany

Abstract

The increased penetration of mobile devices has created opportunities in the health sector and led to emerging of mobile health systems. As much as the mobile health systems have registered tremendous progress, they have been faced with privacy and usability issues. Due to the sensitivity of health information, there is an ethical need to equip mobile health systems with adequate privacy measures. However, these systems should also be useable by the intended users. Even though many researchers are working on solutions, the issues still persist. External factors such as cultural differences have also contributed to the issues, yet they have been under researched. In this article, we conduct a systematic literature review of 22 articles, categorize and present privacy and usability issues and possible solutions. We then discuss the relevance and implications of external factors to the findings on privacy and usability. We end with recommendations to address these external factors.

Keywords

external factors, mobile health systems, privacy issues, security issues, usability issues

Introduction

With the rapid reduction in the cost of mobile devices—especially in developing countries—the likelihood of increased penetration of these devices in the near future is high. Mobile technology has created opportunities in banking, social media, dissemination of information (using bulk SMS) and health systems among others. Mobile health (mHealth) systems are gradually gaining popularity in regard to patient follow-up, communication and lifestyle management. There are a

Corresponding author:
Jane Katusiime, Department of Computer Science, Humboldt-Universität zu Berlin, Unter den Linden 6, 10099 Berlin, Germany.
Email: jane.katusiime@hu-berlin.de

number of mobile devices that have been used in mHealth such as mobile phones (cell-phones and smart phones), tablet computers and mobile internet devices (MID) among others. Despite the availability of various mobile devices as mentioned above and the successful use of these devices in healthcare, this research will focus on mobile phones (cell-phones and smart phones). This is because mobile phones have registered higher user subscription compared to other devices in both developing and developed countries unlike devices like tablets that are more accessible in developed countries.[1,2] In addition, research shows that mobile phones have been used more in mHealth initiatives compared to other mobile devices.[2] It is important to note that wearable technologies such as smart watches have also greatly contributed to healthcare recently and are subject of ongoing research.[3] We will, however, exclude them from this research because they are not highly distributed as mobile phones, especially in low resource settings.[1,4] Much as the mHealth systems have registered tremendous progress, they have been faced with a number of privacy and usability issues such as identity theft, eavesdropping and third-party attacks among others. Different researchers have come up with solutions such as use of access control security models, user authentication and encryption among others but the issues still persist.

Even though it is fundamental to consider privacy and usability of mobile systems, especially mHealth systems that deal with sensitive health information, it remains a challenge to strike a balance between the two. Systems that have emphasized privacy have low usability, while systems focused on usability are less secure.[5] In addition, it is difficult to strike a balance between privacy of users and the desire to monitor communications by, say governments or attackers looking for individual gains. For instance, the terror attacks in the United States led to increased monitoring of communications by the government,[6–8] thus infringing on the rights of individuals. One example case is the USA PATRIOT (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism) Act that was put in place after the September 11 terror attacks to authorize the interception of wired, oral and electronic communications for the production of evidence.[9] There is also an issue of the inevitable trade-off between authenticity versus privacy and anonymity versus accountability.

External factors such as limited application development guidelines and differences in cultures among others have also contributed to privacy and usability issues in mHealth systems. For instance, in some cultures, people consider sharing of mobile devices normal. The sharing phenomenon has reduced the privacy of users, which has in turn negatively impacted on system usability. People who share mobile devices tend to avoid use of mHealth systems that capture sensitive information.[10] This is due to the fear that people with whom they share the devices may have access to their private information.

Due to the sensitivity of health information, there is an ethical need to equip mHealth systems with adequate security measures to safeguard patient's information. However, these systems should also be usable by the intended users. Much as some of the available mobile systems try to strike a balance between security of health information and system usability, there is room for improvement. From the literature review, it is evident that substantial research has been done to address privacy and usability of mobile systems, but fewer researches focus specifically on mHealth systems. There is also limited research addressing privacy in conjunction with usability, and this is evidenced by the limited number of documents from literature that address this issue.. External factors which play an important role in the privacy and usability of mHealth systems have also not been well researched. There is need for more research that addresses privacy issues in conjunction with usability issues in mHealth systems while addressing external factors most, especially in developing countries.

This article is organized into six sections. Section "Methodology" covers the research methodology, and in section "Summary of reviewed literature," we present a summary of the reviewed

literature. In section "Findings from the review," we discuss review findings about privacy and usability issues in mobile systems, external factors that affect privacy and usability and the possible solutions to these issues. This is followed by section "Discussion" that covers our discussion. We end with section "Conclusion and outlook" that entails the conclusion and outlook.

Methodology

In this article, we conducted a systematic review to identify privacy and usability issues in mHealth systems and external factors that affect privacy and usability. A look at the privacy and usability issues in mobile systems in general was done before narrowing down to privacy and usability issues in mHealth systems. The review was done following the procedures of doing literature review which according to Oates[11] include seven procedural steps, that is, searching, obtaining, assessing, reading, evaluating, recording and writing the review.

Search strategy for identification of papers

An electronic database search of peer reviewed papers, open search on websites of reliable institutions and personal contact to authors working in the field was done. The databases searched were PubMed Central (PMC), ACM, IEEE and IRIS; the digital library of World Health Organization's (WHO) published material and technical information. Also, we conducted an open search on websites which included WHO, World Vision International and Vodafone Global Enterprise. Personal information request via email to authors of relevant studies requesting for full texts, additional information and expertise were sent out. In addition, we checked through reference lists of important studies for additional hints.

Search terms were grouped into four categories: privacy specific, usability specific, mHealth systems specific and external factors specific terms. Each category was used as single term or as a combination using operators "AND" and "OR." The following combinations of search terms were used: privacy issues OR usability issues AND mHealth systems AND external factors.

Inclusion and exclusion criteria

Inclusion criteria. Publications on the subject of privacy issues and usability issues in mHealth systems and external factors that affect privacy and usability that are peer reviewed and written in English were included. Reviews of available applications and documentations for particular systems were also included. Only papers published within the time frame of 2001 and 2016 were included because our aim was to look out for the current and relevant issues in mHealth technology which excludes papers that are more than 15 years old due to technological progress.

Exclusion criteria. Studies only mentioned through web pages with limited project information, editorial discussions, summaries of literature for purposes of commentary and papers that are not peer reviewed were excluded.

Search results

Our search identified n = 296 publications, of which n = 250 were from database searches and n = 46 from website searches and personal contacts with authors. In the first round, we excluded n = 114 articles after deletion of duplicates and revision of language and tittles. In the second round, we reviewed the remaining n = 182 publications and excluded n = 160 publications because they

did not meet the inclusion criteria discussed in the previous section. In conclusion, we identified 22 publications that fully met our inclusion criteria and were therefore included in this review.

Summary of reviewed literature

Beach et al.[16] present privacy and security issues associated with location-aware mobile social network systems and solutions to the issues. They use a trusted identity server that uses a cryptographic hash function that allows location-based services to query local mobile devices without disclosing user identity or compromising users' privacy and security. However, Arapinis et al.[17] use formal methods to model and analyze the security properties of 3G protocols by testing major operators such as O2, T-Mobile and Vodafone. They demonstrate the unlinkability and anonymity properties using the automatic verification tool ProVerif. Treese and Stewart[6] propose an architecture where phones manage the end-to-end encryption of the communications while the network handles communications among the wireless devices and wireline carriers without knowing the identity of the users and without persistent identifiers for devices. Bajwa[14] conducts a review of the barriers to adoption of mHealth systems, security concerns that affect these systems and presents ways and means of ensuring security of the electronic health information accessed through mobile devices.

Adhikari et al.[18] carry out a systematic literature review and a comparative analysis of the 20 most popular mHealth apps and provide guidelines for the development of mHealth apps with appropriate security and privacy measures. However, Kotz[19] conducted a literature review of threats to privacy in mHealth technologies and discusses some of the solutions to the identified threats. Vodafone Global Enterprise[20] discuss privacy and security of patient records and mHealth systems and regulation of mHealth systems and devices based on case studies from USA, Europe and Japan. However, Arora et al.[12] discuss privacy and security concerns in mHealth while comparing them to those in cyber security or internet security and present possible solutions. They further discuss federal regulations that affect privacy and security of health information.

Zubaydi et al.[21] Conduct a survey and discuss the security and privacy issues in current mHealth systems and countermeasures to the identified issues. Then, Corallo et al.[22] give an overview of the main privacy and security issues in 3G mobile systems, hotspots context and security issues that may arise by introducing recovery procedures for transactions initiated by mobile users. However, Kainda et al.[5] reviewed current human–computer interaction and security–usability studies and propose a security–usability threat model for conducting security–usability analyses. Johnson and Willey[25] conducted interviews with clinic employees of six healthcare organizations and field research with 10 publically traded healthcare firms to identify usability problems and data leaks in healthcare systems in a peer-to-peer file-sharing network.

Brostoff and Sasse[24] analyzed 10 weeks worth of system logs from a sample of 386 users, whose login attempts were not restricted in the usual manner, and predict that requests for password reminders could be reduced by up to 44 percent by increasing the number of strikes from 3 to 10. Al-Saadi et al.[26] carried out a systematic review of studies on usability challenges and usability testing in mHealth based on studies between 2007 and 2015. They categorize usability issues into application-related challenges and device-related challenges. Then, Mourouzis et al.[28] merged and harmonized reports from students who inspected mHealth applications by means of heuristic evaluation and cognitive walkthrough and presented usability flaws/pitfalls. Zhang and Adipat[29] review studies on usability of existing mobile applications and present issues involved. They propose a generic framework and provide detailed guidelines on how to conduct such usability studies. Cummings et al.[13] examined and used a range of mobile application for health and well-being and discuss security and usability concerns of mHealth systems. They present a consumer-perspective

framework that guides users on how to choose mobile phones and applications. Furthermore, Atkinson et al.[15] discuss personal privacy and vulnerability of individuals and the legal, social and technological perspectives. They ask four mobile phone network providers, Orange, T-Mobile, O2 and Vodafone, to identify some privacy issues and the possible solutions.

Findings from the review

Findings from the review have been discussed in three categories, namely, privacy and usability issues in mHealth systems, possible solutions to the issues and external factors that affect mHealth systems.

Privacy and usability issues

Literature has confirmed that there is a close link between usability and security of mobile system. This poses a challenge of developing mobile systems that are highly secure and at the same time usable.[5] Results from the review further show that there are a number of privacy and usability issues that affect mobile systems, most especially mHealth systems that deal with sensitive patient information. We have summarized the privacy and usability issues in mobile systems in Tables 1 and 2.

We have categorized the privacy issues into identity, access and disclosure issues. We look at identity issues as challenges that emerge as the users try to prove authenticity, for example, through provision of usernames and passwords. However, we look at access issues as challenges that result as the users use the services provided by the system, for example, unauthorized access and having a third party tapping the information exchange as the user interacts with the system. Unlike identity and access issues, disclosure issues have to do with the personal information of the user, for example, as the user tries to transmit information.

Identity issues. K-anonymity is one of the identity challenges which according to Beach et al.[16] results from use of information from an anonymous user to identify his personality without consent. For example, use of someone's preferences such as shared pictures or favorite shopping stores to get his identity. Authentication and linkability attacks are another identity issue common to mHealth systems.[6,17,20] This has to do with who has access to the information in the system, for example, in health systems that support voice collaboration, it may be hard to identify if the person/patient intended to get the information is actually the one being communicated to. Another identity challenge is identity loss, theft or sharing.[5,10–16] Depending on the situation of the users, their identity may be lost or stolen. For example, a user may lose a phone with personal information or a notebook in which access information to systems have been written. In some situations, the user may willingly share identity information, for example, when a user needs information urgently from the system but at that particular time have no access, they may be prompted to share their identity information with another person who is willing to help. All these interfere with privacy of users and the security of the information captured by these systems.

Access issues. Surveys by Beach et al.[16] and Zubaydi et al.[21] identified direct anonymity as one of the access challenges in mHealth systems. Some applications require users to grant access to their private information such as profile details if they are to access and utilize the services provided through the system. Eavesdropping is another major issue in mobile systems according to researchers.[6,14,16,17,21] This ranges from stealing a user's ID and masquerading as that user, intercepting

Table 1. Table showing privacy issues in mobile health system.

Security and privacy issues	Beach et al.[16]	Arapinis et al.[17]	Treese and Stewart[6]	Adhikari et al.[18]	Arora et al.[12]	Atkinson et al.[15]	Kotz[19]	Bajwa[14]	Vodafone Global Enterprise[20]	Zubaydi et al.[21]	Corallo et al.[22]
Identity issues											
Indirect anonymity/ K-anonymity problem	X										
Authentication and linkability attacks		X	X						X		
Identity loss, theft or sharing	X	X	X	X	X	X	X	X	X	X	X
Access issues											
Direct anonymity	X									X	
Eavesdropping	X	X	X			X		X		X	
Third-party attacks						X		X		X	
Denial-of-service attacks										X	
Disclosure issues											
Audit trails			X		X					X	
Data security breaches		X		X	X				X	X	
Unprotected consumer data			X	X						X	X

Table 2. Table showing usability issues in mHealth systems.

Usability issues	Vodafone Global Enterprise[20]	Zubaydi et al.[21]	Johnson and Willey[25]	Zahra et al.[23]	Cummings et al.[13]	Brostoff and Sasse[24]	Al-Saadi et al.[26]	Kumar et al.[27]	Mourouzis et al.[28]	Zhang and Adipat[29]
Accuracy issues										
Memorability and cognition challenges related to authentication		X				X				
Input mechanism and size of screen							X	X	X	X
Efficiency issues										
User's understanding of encryption mechanisms		X								
Slow connectivity									X	X
Low processing power									X	X
Effectiveness issues										
Difficult-to-use user interfaces				X			X	X		
Size of the screen							X		X	
User satisfaction issues										
Un-subjective user assessment		X			X					
Un-secure systems	X	X	X							
Interfacing issue				X			X			

conversations to altering user information among others. Third-party attacks are also prevalent in mobile system.[6,14,21] For example, an mHealth system may be linked to third parties such web servers and insurance companies with whom it shares private patient information, and this may violate the privacy of the user/patient. Sometimes attackers may disrupt flow of information between users, applications and servers leading to denial-of-service attack. According to Zubaydi et al.,[21] denial-of-service attacks create a bigger negative impact in health monitoring systems whose services need to be available all the time.

Disclosure issues. According to the reviewed literature, there are three major disclosure issues affecting mobile systems, that is, audit trails, data security breaches and unprotected consumer data.[6,12,17,18,20–22] Audit trails such as keeping record of who has downloaded the application, ratings of application and billing records may be used to identify and violate the privacy of the users.[6,21] In some instances, medical personal are able to access and view patient records in the mHealth apps without the consent of the patients.[18] In addition, some applications have trackers that track user behavior,[21] and all these may lead to breach of data security. Most of the applications do not encrypt the data entered by the users,[18] for example, an intruder can know what the user is suffering from by just looking at what application the user is using and then check out the details in the app. In addition, applications with a voice call function show telephone numbers to call recipients which intruders may use to map to user's information. Furthermore, transmission of information is often over airwaves that are not protected,[22] and all these may lead to disclosure issues in mobile systems.

Usability issues

We have divided and discussed usability issues in four categories, that is, accuracy, efficiency, effectiveness and user satisfaction as summarized in the table below.

According to Kainda et al.,[5] usability can be looked at in four categories, that is, effectiveness, accuracy, efficiency and user satisfaction. While efficiency focuses on the amount of time the user takes to complete a task, accuracy is concerned with how accurate the information input in the system is. However, effectiveness focuses on the ability of the user to do a task while satisfaction looks more into the user's acceptance of the system. There are a number of issues that affect usability of mobile systems as summarized in the table above and discussed below.

Accuracy issues. One of the major accuracy issues is memorability and cognition challenges related to authentication.[5,24] In most cases, users are required to input their authentication details such as usernames and passwords with 100 percent accuracy. Moreover, some systems require use of passwords that are a combination of numeric, text and other complex characters aiming at enhancing the security of user information. However, memorizing such passwords may be difficult, especially if the users have many of such systems they are using. This may prompt the user to frequently request for resetting of passwords or write them down, which may lead to privacy threats. The screen size and input mechanisms of mobile devices may also interfere with the accuracy of input data.[26,28] Mobile devices have small screens and in most instances have tedious input mechanisms which may interfere with the accuracy of information the user inputs. For example, some mobile devices have small buttons which also have various input functions whereby a user may mistakenly press two or more buttons at the same time leading to inaccurate data inputs. Moreover, the user may be required to press a similar button many times to get a certain input, in cases where the input is encrypted such as passwords, the user may end up inputting inaccurate data.

Efficiency issues. A slow or fast connectivity may determine the efficiency of a system. Mobile devices often have slow connectivity which in some cases is unreliable,[28,29] and this negatively impacts applications that rely on connectivity, most especially mHealth applications that deal with real-time critical information exchange. Also, processing power of a device may determine the efficiency of the applications it runs. Mobile devices are characterized by low processing power,[28,29] and this increases the amount of time the user takes to complete a task. This may render some applications inefficient and worse still unusable on devices with very low processing power.

Effectiveness issues. In a systematic review of usability and testing challenges in mHealth by Al-Saadi et al.,[26] difficult-to-use user interface was ranked as the biggest usability challenge followed by screen size of the devices. User interfaces allow the user to interact with the system, and therefore, if they are poorly designed, they may render the applications unusable. For instance, if the interfaces have no help function to guide the user on the format of the data required such as dates and no meaningful error correction prompts, the user may find it hard to complete some tasks. In addition, if the interfaces require a lot of data input, bearing in mind the size of the screen and input mechanism of mobile devices, the user may not be able to complete some of the tasks.

User satisfaction issues. User assessment that is not subjective is one of the issues that may hinder usability of an application.[5,13] Regardless of how effective or efficient the system is, user satisfaction determines whether the system will be used or not. It is, therefore, paramount for users to do a subjective assessment of the application before it is put into use. In addition, how secure the application is and the ability of the user to identify secure systems also contributes to user satisfaction.[5,20,25] Applications that the users perceive as secure are more likely to be acceptable to users who intend to keep their data private, most especially applications that deal with sensitive patient information. Furthermore, interfacing issue is another usability issue presented by health practitioners. They categorize it into two forms, that is, complexity of interfacing with the technology and limited interface with patients.[23,26] Health practitioners report reduced physician–patient interfacing when using mHealth systems and how this may negatively affect their physician–patient relationships and reduce their satisfaction. Also, complex systems require a lot of training time and may increase work load for the physicians when trying to navigate the systems.[23]

External factors that affect privacy and usability of mHealth systems

There are a number of external factors that affect privacy and usability of mHealth systems. Scarcity of mHealth policies, strategies and standard guidelines for development of mHealth applications and failure to enforce the few that are available is one of these factors. Most countries have no mHealth policies and strategies, for instance, in a health debate series by Vodafone Global Enterprise,[30] of all countries worldwide, only one-quarter have a national policy or strategy on telemedicine. Enforcement is also lacking. This is evidenced by some developers who tend to ignore privacy measures such as authentication which may be a vital requirement for all mobile systems that deal with sensitive information. For instance, in a review of 20 most popular mHealth applications by Adhikari et al.,[18] only two apps (10%) required the user to provide user authentication information before login. Another review of 19 mHealth applications for iOS, Blackberry and android devices by Kharrazi et al.[31] also found that seven of the applications had no security measures for user authentication. Lack of user authentication may lead to issues like eavesdropping and identity theft among others. Moreover, some developers share user information with third parties, in some cases without the user's knowledge/consent. In the same review by Rajindra et al., 13 apps (65%) out of the 20 that were reviewed shared user information with third parties such as

advertisers. This may lead to data security breaches, increase in third-party attacks and linkability attacks among others.

However, some countries with established policies and guidelines for eHealth also have a unique set of challenges when it comes to privacy and usability of mHealth systems. For instance, as a result of frequent terror attacks, some countries have developed national security legislations that may permit surveillance which may go as far as accessing personal information such as health information of individuals in case of suspicion.[6,32,33] A good example is in the United States where the government can impose a mandatory implementation of eHealth systems in some departments and may have access to health information when the need arises.[33] This increased monitoring by governments violates the privacy of people and may hinder individuals from using health applications due to fear of having their sensitive health information accessed by the authorities. In addition, some countries have regulations and guidelines that only cover a subset of mHealth applications. For example, the Food and Drug Administration (FDA) in the United States only regulates applications that are likely to pose a risk to patients' safety if they do not function as intended.[7] This leaves out applications designed for record archiving, retrieving and sharing. As a result, users may not trust the credibility of these unregulated applications and then avoid using them.

Furthermore, while most developed countries have legal provisions for use of electronic health systems such as mHealth systems, most developing countries have no privacy and data protection laws, which makes patient's information vulnerable to third-party attacks.[12,15,34] This vulnerability may hinder users from using mHealth systems due to the fear of having their privacy violated.

In addition, cultural differences also affect privacy and usability of mobile systems.[28,35] For instance, in some cultures, sharing of mobile devices is considered normal, and as a result of this sharing phenomenon, information sent to or/and stored on a shared device may end up being accessed by people for whom it was not intended. As a result, this sharing phenomenon may discourage a user of a shared device from using an application, especially if that application captures sensitive information such as health information that the user may prefer to keep private.

Human factors such as age, personality, literacy level and cognitive ability also play an important role in usability of systems.[20,28,36] For instance, systems that appeal to the young age brackets may not appeal to the older age brackets. Likewise, the design of systems meant for people with low literacy levels or people with cognitive challenges may have requirements that may not apply to systems meant for people with higher levels of education and good cognitive abilities. For example, a system developed for people who cannot read and write may not utilize text formats, but rather use audio, video and pictorial formats while systems meant for literates may utilize text and all the other formats. These human factors determine difficulty or ease with which a user will interact with the application and consequently may influence the acceptability of the application.

Finally, economic situations and poor infrastructure may hinder usability of mHealth systems.[10] For example, in some rural settings in developing countries, there is limited access to network connection which may limit use of applications that depend on network connection. In addition, poor network hinders implementation of mHealth application, a case in point is the HMRI project in India that had 50 percent of its services via call centers interrupted due to network issues.[37] Furthermore, some areas are characterized by power shortages. This implies that people in these areas may not be able to charge their mobile devices and use them all the time. In rural areas, especially in developing countries where there is no power or power is unreliable, people charge their mobile devices at charging centers in trading centers or towns that have generators or other reliable power sources. This means that these people have no access to their devices during the time when these devices are at the charging centers. This may discourage owners of these devices from using applications that require the user to have access to the device all the time. In addition, applications

that deal with sensitive information such as health information may be avoided by these possible users because the security of the information and the devices while at the charging centers may be questionable.

In order to reduce privacy and usability issues in mHealth systems, there is need to address external factors that have been found to have a negative impact as discussed above. This may increase privacy of users and in the long run increase acceptability and usability of mHealth systems.

Possible solutions to privacy and usability issues

We have categorized the solutions based on the issues they deal with, that is, solutions to identity, access and disclosure issues (privacy issues) and solutions to accuracy, efficiency, effectiveness and user satisfaction issues (usability issues) as summarized in Table 3.

Solutions to identity, access and disclosure issues (privacy issues). Researchers and developers have come up with solutions to privacy issues[6,12,16–22] discussed above. Among the popular solutions is encryption,[14,15,17–20] which according to Adhikari et al.[18] refers to a method of data protection, whereby data are converted into a form that unauthorized persons cannot easily understand. Encryption may be used to reduce problems such as eavesdropping and K-anonymity among others. Encryption can be achieved by encryption of the data handled by the system or encryption at the process level. Another popular solution is the use of authentication,[12,18–22] such as use of usernames and passwords. Some have gone further to use double-factor authentication,[20] whereby more personal information such as favorite pet name is requested from the user to ensure that even when the first level of authentication is broken by a hacker, the personal information may provide a second level of security. This can solve issues like eavesdropping, identity theft and denial of service attacks among others.

According to some researchers,[6,18,21] erasing identity, remote wiping and disabling may reduce privacy issues in mHealth systems. For example, when the user's phone is lost or stolen, the user should be able to remotely erase or disable access to the data on that phone. This can go a long way in eradicating issues like third-party attacks, audit trials and identity loss, theft or sharing among others. In addition, researchers emphasize access control through use of access control security models such as role-based access control (RBAC) which limits access to data to legitimate entities using the mHealth systems.[6,18,19] This may reduce challenges of eavesdropping, data security breaches and the issue of unprotected consumer data. Use of firewalls and avoiding unsecure Wi-Fi connections may also increase privacy in systems.[12,14,18] Unsecured Wi-Fi networks pose a risk of interception from intruders. However, personal firewalls can intercept and block malicious connections. Beach et al.[16] also propose use of logic simplification algorithms, anonymous identifiers and identity servers to reduce access threats.

Solutions to accuracy, efficiency, effectiveness and user satisfaction issues (usability issues). User involvement and iterative design are some of the solutions to usability issues.[5,28] This involves improving versions of the system based on the feedback from users. The researchers emphasize subjective assessment of systems by the users in order to increase acceptability and use of usage scenarios and threat scenarios to reduce issues like difficult to use user interfaces.[5] In addition, appropriate testing could reduce usability issues[5,26,28] related to user satisfaction and un-subjective user assessment. However, a study by Brostoff and Sasse[24] suggests that increasing the number of login attempts may reduce memorability and cognition challenges related to authentication and this may increase usability. According to the same research, the current policy applied to

Table 3. Table showing possible solutions to privacy and usability issues in mHealth systems.

Possible solutions	Atkinson et al.[15]	Beach et al.[16]	Arapinis et al.[17]	Arora[12]	Treese and Stewart[6]	Adhikari et al.[18]	Kotz[19]	Bajwa[14]	Vodafone Global Enterprise[20]	Zubaydi et al.[21]	Corallo et al.[22]	Kainda et al.[5]	Johnson and Willey[25]	Brostoff and Sasse[24]	Al-Saadi et al.[26]	Mourouzis et al.[28]
Solutions to identity, access and disclosure issues																
Encryption	X		X	X		X	X	X	X		X					
User authentication, for example, passwords				X		X	X		X	X	X					
Erasing identity, Remote wiping and disabling					X	X		X		X						
Access control security models, for example, RBAC					X	X	X									
Avoid unsecured Wi-Fi connections				X		X										
Use firewalls	X					X		X								
Solutions to accuracy, efficiency, effectiveness and user satisfaction issues																
User involvement and iterative design												X				X
Higher processing power																
Appropriate testing												X			X	X
Password resetting														X		
Better input mechanisms																X
Increase login attempts														X		
Increase screen size															X	
Reduce input to be typed																X

RBAC: role-based access control.

passwords grants users three false login attempts after which the user is blocked. There has been an increase in the screen size of mobile devices in order to improve the input mechanisms.[26,28] This has been evidenced by the continuous increase in the size of smart phones by the different manufacturers. For instance, the current Samsung smart phones are much bigger than the initial Samsung Galaxy S.[38] In addition, reducing the amount of data input may increase usability.[28] Some developers have adapted mechanisms of reducing the amount of data the user has to manually input into the system, for example, using drop-down menus to make interaction with the system less tasking.

Discussion

The review identified a number of issues that affect privacy and usability of mHealth systems. It also uncovered some solutions that may be used to minimize these issues as discussed in the previous sections. However, there are also some issues that have no solution yet. The findings show that there is a trade-off between system privacy and usability. Emphasis on privacy leads to development of unusable systems, while emphasis on usability reduces the security component of the system. There is extensive research on the solutions to privacy and usability of systems compared to the research on striking a balance between privacy and usability. Findings of the review indicate that external factors play a significant role in the design and acceptability of mHealth systems which consequently affect privacy and usability of these systems. For instance, an external factor like literacy levels may influence privacy and usability of mHealth systems as discussed under the section on external factors. However, there is limited research on how to tackle the factors in conjunction with striking a balance between privacy and usability of mHealth systems. This is evidenced by the limited literature about the same.

All the nine privacy issues identified under identity, access and disclosure issue categories in Table 1 had solutions. The solutions range from data and process encryption, user authentication, use of firewalls and access control security models among others. Some solutions could be used to address more than one issue. For instance, use of data and process encryption was shown to reduce privacy issues such as eavesdropping, identity theft and linkability attacks, while user authentication such as use of usernames and passwords was shown to reduce denial of service attacks and indirect anonymity problem among others.

However, the review identifies solutions to usability issues that differ from the ones of privacy. The solutions may be looked at in terms product usability solutions and process usability solutions. Process usability solutions include user involvement, iterative design, appropriate system testing among others while product usability solutions include criteria and guidelines that ensure product usability in terms of reliability, ease to learn, easy memorability and few errors among others. Some solutions also address more than one issue just like the case of solutions to privacy issues discussed above. For instance, user involvement and iterative design may eliminate user interfaces that are not easy to use and increase user satisfaction.

Based on the review, privacy issues and usability issues in mobile systems in general have been widely researched and to some extent have concrete solutions. However, fewer researches have focused on mHealth systems specifically. There is limited research on privacy in conjunction with usability in mobile systems and most especially in mHealth systems where these concepts are fundamental. Moreover, the existing research approaches that tried to address the issue of striking a balance between privacy and usability in mobile systems did not focus on mHealth. The remaining few that look at mHealth systems are based on the context of developed countries. That research cannot often be used as a model for developing countries because of the difference in external factors such as infrastructure and cultural differences among others. For instance, while

it may not be common to share mobile phones in developed countries, it is a common practice in low income and middle income families in developing countries. This sharing phenomenon poses a new set of privacy and usability issues that require solutions different from those applied in developed countries. The limited research poses a challenge of how to develop mHealth systems that are highly secure and at the same time usable, most especially in developing countries. More research is needed here.

Much as literature identifies many external factors that affect privacy and usability of mHealth systems and confirms that dealing with external factors may increase usability of mHealth systems and may also improve privacy of the user, it provides few solutions to these issues. As one of our contributions, we propose solutions to deal with external factors.

One of the ways of dealing with external factors is by improving awareness and offering training to users regarding privacy, security and usability of mHealth systems. For instance, implementation of security measures and letting the users know what, how and where their data are stored may increase acceptance. Second, applying principles of user-centered design which according to Oates[11] refers to the involvement of users in all phases of system development may also help in avoiding most of the privacy and usability issues. In this case, feedback from users should be put into consideration in the various iterative levels of system development. Involvement of users is more likely to lead to development of applications that are acceptable and increase user satisfaction, which in the long run reduces acceptability and user satisfaction issues. In addition, appropriate system testing should also be done. Testing ranging from functionality testing to usability testing using both formal and informal methods need to be emphasized. Furthermore, all stakeholders raging from policy makers, manufacturers to health workers among others should be indulged in order to come up with security standards, system development guidelines and infrastructures that support privacy and usability of mHealth systems.

Conclusion and outlook

There is considerable research on privacy issues and usability issues in mobile systems in general but relatively fewer in mHealth systems. There are also a number of possible solutions to these issues as discussed in the previous sections. However, with the small number of documents in the literature combining privacy and usability, it appears that less is being done in addressing ways of striking a balance between privacy and usability of mHealth systems. External factors, which according to the review, influence privacy and usability of mHealth systems are also under researched. There is a need for more research on how to increase privacy in mHealth systems while considering usability. There is also need to address external factors, especially in the context of developing countries where, for instance, mobile devices may be shared.

Access control security models such as RBAC have been shown to address some security issues such as eavesdropping, which improves security of mobile systems. Much as they have to a greater extent been utilized in mHealth systems, they have major limitations as highlighted by Tolone et al.[39] In an attempt to bridge the gap in research on privacy and usability, in the next research, we shall focus on security models that are currently used to ensure privacy of users and focus on how to improve them to encompass and enhance the issue of usability of the systems, especially mHealth systems. Since external factors such as literacy levels and cultural differences among others have also been sighted to negatively affect security and usability of mobile systems, we will focus on cultural factors, and in this regard, we will specifically focus on the culture of sharing devices, especially in developing countries where this phenomenon is common. So, we shall look at the possibility of developing a security model that can strike a balance between security and usability while taking into consideration the specified external factor.

Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship and/or publication of this article.

References

1. World Health Organization. *From innovation to implementation—eHealth in the WHO European region*. Geneva: WHO.
2. Ventola CL. Mobile devices and apps for health care professionals: uses and benefits. *PT* 2014; 39: 356–364.
3. Piwek L, Ellis DA, Andrews S, et al. The rise of consumer health wearables: promises and barriers. *PLoS Med* 2016; 13: 1–9.
4. Mohapatra DP, Mohapatra MM, Chittoria RK, et al. The scope of mobile devices in health care and medical education. *Int J Adv Med Heal Res* 2015; 2: 1–8.
5. Kainda R, Fléchais I and Roscoe AW.Security and usability: analysis and evaluation. In: *2010 international conference on availability, reliability and security, Krakow*, 15–18 February 2010, pp. 275–282. New York: IEEE.
6. Treese GW and Stewart LC. An architecture for security and privacy in mobile communications. Arxiv.org, 2001, https://arxiv.org/abs/cs/0110042
7. Boulos MNK, Brewer AC, Karimkhani C, et al. Mobile medical and health apps: state of the art, concerns, regulatory control and certification. *Online J Public Health Inform* 2014; 5: 229.
8. NIST. NIST special publication 800-53A, R4: assessing security and privacy controls in federal information systems and organizations: building effective assessment plans, 2014, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf
9. Public Law. Uniting and strengthening America by providing appropriate tools required (USA PATRIOT Act) act of 2001.
10. Aranda-Jan CB, Mohutsiwa-Dibe N and Loukanova S. Systematic review on what works, what does not work and why of implementation of mobile health (mHealth) projects in Africa. *BMC Public Health* 2014; 14: 188.
11. Oates BJ. *Research information systems and computing*. Thousand Oaks, CA: SAGE, 2006.
12. Arora S, Yttri J and Nilse W. Privacy and security in mobile health (mHealth) research. *Alcohol Res* 2014; 36: 143–151.
13. Cummings E, Borycki EM and Roehrer E. Issues and considerations for healthcare consumers using mobile applications. *Stud Health Technol Inform* 2013; 183: 227–231.
14. Bajwa M. mHealth security. *Pakistan J Med Sci* 2014; 30: 904–907.
15. Atkinson S, Jagodzinski P, Johnson C, et al.Personal privacy: exploitation or control through technology. In: *Proceedings of the sixth international network conference* (INC2006), Plymouth, 11–14 July 2006, pp. 269–276. Plymouth: CSCAN.
16. Beach A, Gartrell M and Han R.Solutions to security and privacy issues in mobile social networking. In: *Proceedings of the 2009 international conference on computational science and engineering*, Vancouver, BC, Canada, 29–31 August 2009, vol. 4, pp. 1036–1042.
17. Arapinis M, Mancini L, Ritter E, et al.New privacy issues in mobile telephony: fix and verification. In: *Proceedings of the 2012 ACM conference on computer and communications security*, Raleigh, NC, 16–18 October 2012, pp. 205–216. New York: ACM.
18. Adhikari R, Richards D and Scott K. Security and privacy issues related to the use of mobile health apps. In: *Proceedings of the Australasian conference on information systems (ACIS 2014)*, Auckland, New Zealand, 8–10 December 2014. Auckland, New Zealand: Auckland University of Technology.

19. Kotz D. A threat taxonomy for mHealth privacy. In: *Proceedings of the 3rd international conference on communication systems and networks (COMSNETS 2011)*, Bangalore, India, 4–8 January 2011. New York: IEEE.
20. Vodafone Global Enterprise. *Evaluating mHealth adoption barriers: privacy & regulation 2013*. London: Vodafone Global Enterprise.
21. Zubaydi F, Saleh A, Aloul F, et al. Security of mobile health (mHealth) systems. In: *Proceedings of the 2015 IEEE 15th international conference on bioinformatics and bioengineering (BIBE)*, Belgrade, 2–4 November 2015, pp. 1–5. New York: IEEE.
22. Corallo A, Cremonini M and Damiani E. Security, privacy, and trust in mobile systems. *Mobile and Wireless Systems beyond 3G: Managing New Business Opportunities*. 2005, pp.312–340.
23. Zahra F, Hussain A and Mohd H. Usability factors of mobile health application for chronic diseases. *AIP Conf Proc* 2016; 1761: 020108.
24. Brostoff S and Sasse MA. Login attempts can improve password usability. *Computer* 1–4.
25. Johnson ME and Willey N. Usability failures and healthcare data hemorrhages. *IEEE Secur Priv* 2011; 9: 35–42.
26. Al-Saadi TA, Aljarrah TM, Alhashemi AM, et al. A systematic review of usability challenges and testing in mobile health. *Int J Account Financ Report* 2015; 5: 1.
27. Kumar S, Nilsen W, Pavel M, et al. Mobile health: revolutionizing healthcare through transdisciplinary research. *Computer* 2013; 46: 28–35.
28. Mourouzis A, Chouvarda I and Maglaveras N. mHealth: common usability and user experience practices and flaws. In: *Proceedings of the European, Mediterranean & Middle Eastern conference on information systems*, Athens, 1–2 June 2015, pp. 1–16, http://pincloud.med.auth.gr/pubs/P9_11.pdf
29. Zhang D and Adipat B. Challenges, methodologies, and issues in the usability testing of mobile applications. *Int J Hum Comput Interact* 2005; 18: 293–308.
30. Vodafone Global Enterprise. *Evaluating mHealth adoption barriers: politics and economics*. London: Vodafone Global Enterprise, 2013.
31. Kharrazi H, Chisholm R, Van Nasdale D, et al. Mobile personal health records: an evaluation of features and functionality. *Int J Med Inform* 2012; 81: 579–593.
32. World Health Organization and International Telecommunication Union. National eHealth strategy toolkit, 2012, pp. 1–2, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-E_HEALTH.05-2012-PDF-E.pdf
33. Office of the National Coordinator for Health Information Technology (ONC), Department of Health and Human Services. Health information technology: standards, implementation specifications, and certification criteria for electronic health record technology, 2014 edition; revisions to the permanent certification program for health information technology. Final rule. *Fed Regist* 2012; 77: 54163–54292.
34. Kay M, Van Andel MO-G, Tristram C, et al. eHealth tools & services: needs of the member states. Report of the WHO Global Observatory for eHealth (WHO/EHL/06.1), 2006, http://apps.who.int/medicinedocs/documents/s16468e/s16468e.pdf
35. Avancha S, Baxi A and Kotz D. Privacy in mobile technology for personal healthcare. *ACM Comput Surv* 2012; 45: 1–56.
36. Frisbee KL. Variations in the use of mHealth tools: the VA mobile health study. *JMIR Mhealth Uhealth* 2016; 4: e89.
37. Ivatury G, Moore J and Bloch A. A doctor in your pocket-health hotlines in developing countries. *Innov Winter* 2009; 4(1): 119–153.
38. Al-Ismail M and Sajeev ASM. Usability challenges in smartphone web access: a systematic literature review. In: Liu K, Gulliver SR and Li W (eds) *Service science and knowledge innovation*. Berlin: Springer, 2014, pp. 459–470.
39. Tolone W, Ahn G-J, Pai T, et al. Access control in collaborative systems. *ACM Comput Surv* 2005; 37: 29–41.