Proceedings of the 53rd Hawaii International Conference on System Sciences | 2020

Health Information, Human Factors and Privacy Issues in Mobile Health Applications

Wagner Silva
Federal University of
Rio de Janeiro State - UNIRIO
Oswaldo Cruz Foundation - Fiocruz
wagner.silva@uniriotec.br
wagner.silva@fiocruz.br

Carolina Sacramento
Federal University of
Rio de Janeiro State - UNIRIO
Oswaldo Cruz Foundation - Fiocruz
carolina.sacramento@uniriotec.br
carolina.sacramento@fiocruz.br

Edenildo Silva
Federal University of
Rio de Janeiro State - UNIRIO
edenildo.silva@uniriotec.br

Ana Cristina
Bicharra Garcia
Federal University of
Rio de Janeiro State - UNIRIO
cristina.bicharra@uniriotec.br

Simone Bacellar
Leal Ferreira
Federal University of
Rio de Janeiro State - UNIRIO
simone@uniriotec.br

Abstract

Recent innovations on mobile technologies combined with the widespread use of mobile devices have allowed for a new perspective on health care applications: mobile health applications (m-Health). Ensuring information privacy while delivering the expected vital signs monitoring is still a challenge for the adoption and use of these applications. Most research focuses on methods and techniques to prevent unauthorized access of personal information in the context of mHealth; our research considers the m-Health user's point of view. From a systematic literature review in the Computer Science literature, we identified the main users' demands concerning privacy. There are different types of privacy issues with different types of proposed solutions. Users' privacy preferences and information sharing issues are emphasized showing the counterpoint for privacy. Our objective in this paper is to contribute towards a better understanding of the trade-offs between users' desires and privacy concerns with regard to the adoption of the m-Health technology, identifying issues that need to be addressed in order to reduce users' concerns about privacy in m-Health.

1. Introduction

Mobile health applications, or m-Health, are applications delivering medical information or support using wireless mobile devices such as mobile phones, wearable monitoring devices and personal digital assistants (PDAs) [1]. Mobile health is a special type of electronic Health application (e-Health) using mobile devices already incorporated into people's daily lives. In general, m-Health applications require the ability to monitor users' activities and behaviors to enable personalized medical care.

The widespread use of mobile technologies combined with the need for personalized and lower-cost health care have fostered the emergence of m-Health technology. It is an opportunity to deliver health services with innumerable potential benefits such as: constant monitoring of health, accuracy of diagnoses and prevention of new problems, reduction of health service costs, availability of care for people living in remote areas, improvement in physician-patient communication, among others.

Despite these potential benefits, the sensitive nature of the personal information circulating in these mobile applications brings up privacy concerns and consequences that have led to people becoming very concerned about privacy. People are reluctant to share information about their health with their families through mHealth applications for many reasons. They are concerned, for instance, that family members might judge them and even reprimand them because of their physical condition and fitness [2]. Another reason is that many people do not want to concern their family because of their current health condition. In the workplace the concern is about being disqualified in a selection process for a higher position, also because of one's health condition. Other factors that worry people about having their health data available in mHealth

URI: https://hdl.handle.net/10125/64162
978-0-9981331-3-3

applications are cases of diseases that bear a social stigma. For example, a patient with controlled epilepsy may be prevented from driving even if their disease is under control.

Privacy is the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them should be communicated to others [3]. It is an abstract and subjective concept, linked to each individual's perception of what constitutes a threat to their personal property or physical or moral integrity, depending on cultural aspects (such as religion, tradition, customs, education, etc.) and more subjective issues, such as age, health status, current context [4, 5].

With the arrival and rise of the Internet and new perspectives on interaction and communication between individuals, people have come to face an increasing amount of decisions about the privacy of their information in particular social setting[6]. There are decisions regarding different aspects, from aspects of visibility settings in social networks to aspects focused on how to download a smartphone application in accordance with confidential data that this scenario requires [7].

Many privacy researches regarding mHealth in literature are concerned with the technical aspects of privacy related to ensuring the security of information transmitted over mobile networks and stored on the device or in cloud services to prevent unauthorized access of a patient's information [8, 9, 10]. Nevertheless, the collaborative use of m-Health technology for shared care management presents other privacy demands related to human factors such as the desires and preferences of the user in sharing their health information with authorized entities [11].

The objective of this paper is to contribute towards a better understanding of the trade-offs between users' desires and privacy concerns with regard to the adoption of m-Health technology, identifying issues that need to be addressed in order to reduce users' concerns about privacy in mHealth. We looked 109 papers in the field of Computer Science, selected between 2012 and 2018, focusing on human factors in order to identify which users' privacy demands the research has dealt with, which solutions have been proposed so far and what are the trade-offs of m-Health.

2. Related works

The interest for privacy in computer systems is not a recent concern. In 1969, Hoffman [12] was already discussing user access control strategies and information privacy for existing systems. He saw the efficiency of storing personal information in contrast to the dangers of third party access to such information. The author reviewed the legal and administrative safeguards for the protection of sensitive information on computers and the technical solutions that were proposed at the time. In his conclusion, Hoffman cited another author (Paul Baran) who mentions the responsibility of computer engineers to preserve people's right to privacy.

This work proposed by Hoffman [12] considered the technical perspective, without taking into account the user's point of view. A recent study focused on privacy-related human factors was produced by Barth and Jong [13] who conducted a systematic literature review to understand the paradox of online privacy; users claim to be very concerned about their privacy, but do very little to protect their personal data. After reading 32 complete articles, Barth and Jong [13] identified 35 theoretical approaches to decision-making, concluding that the paradox has different perspectives, distinguishing decision making according to rational and irrational risk-benefit calculations and the context in which the privacy paradox occurs [13]. These issues are nothing new, they were addressed by Pavlou in 2011 where the privacy paradox was described in his reviews on information privacy as the phenomenon where an individual expresses strong privacy concerns but behaves in a way that contradicts these concerns. For example, despite self-reported privacy concerns, some consumers still share their personal information[14].

Even after considering the user's point of view, Aimeur [15] addresses the issue of how to reach the delicate balance between privacy and user personalization, mentioning that nowadays, more and more users need to keep control over their personal data by fine tuning their applications' default settings. The author also claims that mobile health would greatly benefit from users' direct control, choosing when, where and with whom to share their personal data[15].

The work produced by de Kotz in 2016 gives an overview of privacy and security in the context of mHeath, from the challenges, data sharing, privacy, APPs and security. In his work the author concludes that the user must have the autonomy to decide how, when and with whom to share, which data and at what level of granularity in order to make them feel safe when using mHealth apps [16].

3. Methodological procedures

In order to reach the proposed goal, this study used the Systematic Literature Review (SLR) method proposed by Barbara Kitchenham [17] for Software Engineering research. This method involves three

phases: planning, conducting and reporting the results; the latter is summarized into communicating the results of the review that is the main objective of this paper.

3.1. Planning

At this stage, we defined the objective of the systematic review, the research questions to be answered (main and specific), and indeed the entire protocol of the review.

The purpose of the review was to contribute with a general overview on Computer Science research related to privacy of m-Health technologies, in terms of users' privacy preferences and desires, from 2012 to 2018. We chose to investigate the field of computer science because research in this area usually addresses the technical issues of privacy, without considering the user's point of view, as in the work of Agarkhed[18], Guilln-GMez[19] and Plachkinova[20].

Avancha [11] and Els[21] identify relevant topics on privacy from a broad point-of-view. The findings includes adopted technologies and open questions, mainly in relation to human factors. The present research adds knowledge when mapping Computer Science literature, searching for works that address privacy specifically from the point of view of human factors. To this end, the following (main and specific) research questions were defined:

Main question: "*What are the main issues addressed and solutions presented by the Computer Science community in recent years (2012-2018) about the user's privacy in m-Health technologies from the user's perspective*".

Specific Questions (SQ):

- **SQ1**: What types of privacy threats are considered in the research?
- **SQ2**: What user privacy demands are considered in the research?
- **SQ3**: What correlation between environment context and users' privacy preferences is considered in the research?
- **SQ4**: What health domain is addressed in the research?
- **SQ5**: What solutions have been proposed to address privacy issues from the user perspective in the research?
- **SQ6**: What target audience is considered in the research?

Our systematic review created a query string following the PICOC method, the acronym for **Patient** (m-Health, mHealth or Mobile health), **Intervention** (Information privacy solutions, human factors, user issues), **Comparison**, (Include, if any), **Outcomes** (User perception, satisfaction and requests) and **Context** (Computer Science) [22].

We decided not to add other terms to the string generated by PICOC keywords, after a calibration step, to include literature of a broader scope. This decision was important to achieve more expressive results in search, since the addition of new terms significantly limited the number of articles returned in the databases tested. After calibration, the following search string was defined:

((m-health OR "mobile health" OR mHealth) AND privacy)

The database sources were ACM Digital Library, IEEE Xplorer, and Scopus, which were chosen because they form the main publication base in the computer science area. The first and second databases were selected to provide comprehensive coverage on the Computer Science field. Scopus was chosen due to the fact that it is one of the largest abstract and citation databases of peer-reviewed literature in the world.

The time period considered was from 2012 to 2018 because the work of Avancha [11] presented an extensive (non-systematic) literature review conducted in the years prior to 2012, identifying a number of open research questions about privacy, and some regarding human factors in m-Health.

In selecting the articles, we established filters directly on the database search forms, such as search only in the title, abstract and keyword fields. We also filtered papers in English only and restricted to the area of Computer Science. Whenever possible, we filtered only papers from journals, conferences (full papers) and book chapters directly on the database extraction form.

Table 1 shows the inclusion and exclusion criteria defined for the screening step.

3.2. Conducting

In this phase, the papers were (1) taken from the databases, using query string and filters previously mentioned, (2) pre-selected after a fast screening on the abstract text and (3) synthesized after full reading.

In the screening step, each of the evaluators was responsible for reading the title and abstract of the papers from a specific database. Before starting the reading, we used an automatic feature present in Parsifal

Table 1. Inclusion and exclusion criteria

Inclusion criteria
1. **On target**: The paper focuses on privacy issues from the users' perspective; **and** 2. **On target**: The paper focuses on m-Health technology.
Exclusion criteria
1. **Out of the focuse**: The paper does not consider the user's perception concerning information privacy; **or** 2. **Out of the topic**: The paper does not address information privacy in m-Health applications; or 3. **Content not robust**: The paper is in the form of an editorial, keynote, abstract, short paper, tutorial, poster and similar; **or** 4. **Out of the focus**: The paper only addresses the technical aspects of privacy, such as, data transmission, encryption and cloud storage; **or** 5. **Repeated**: The paper does not present new material; it is only a more concise/extended version of the same material. Only the most recent was considered.

software to identify the duplicate records.

We adopted two evaluators at this stage, i.e., for each rejected paper, a second evaluator should analyze it. When an article rejected by the first reviewer is selected by the second reviewer and there is a conflict between reviewers, a third reviewer validates as a meta-review. This procedure was used to ensure a better quality of screening. In the first round of screening, 97 articles were selected. After a second analysis, the number of articles increased to 109. This happened because 12 articles that had been rejected were selected by a second reviewer and validated by the meta-review in the event of a conflict.

Later, in the Eligibility step, we performed a full reading of the 109 pre-selected articles (also using two evaluators) and discarded 88 papers, in most cases because they were within the exclusion criteria 80 papers) or because we didn't have access to the full text (8 papers). The 21 eligible articles were analyzed and synthesized in a way that was able to answer the established research questions.

Figure 1 illustrates the systematic review flow, presenting the total of articles included and excluded at each stage. It is an adaptation of the PRISMA Flowchart, proposed to report the results of a systematic literature review [23].

4. Results and discussion

The 21 articles resulting from the SLR were classified into descriptive and comparative axes related

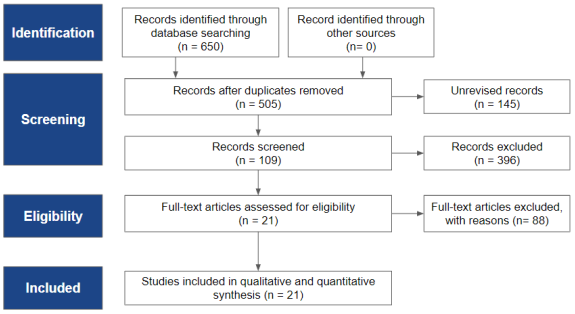

Figure 1. Systematic review flow

to the research questions established in the planning stage of the systematic review. In the next sub-sections, we present the results obtained and discussions for each axis.

4.1. Types of threats to privacy (SQ1)

Table 2. Distribution and percentage of articles by type of threat to privacy. In some papers, more than one type was identified, so total is greater than 100%

Threats to privacy	**Related papers**	**%**
Access permissions	[24] [16] [2] [25] [26] [27] [28] [29] [30] [21] [31] [32] [11] [33] [34] [35] [36]	85.7
Improper information disclosure	[37] [16] [2] [25] [34] [26] [28] [35] [21] [32] [11] [33] [38] [30]	66
Anonymity Loss	[16] [35] [11] [33]	19
Device compromised, lost or stolen	[35] [30] [21] [11] [28]	23.8
Disclosures about device presence	[11]	4.8
Service provider reliability	[26] [35] [31]	14.3

It's possible to observe in Table 2 that one article addresses various types of privacy threats. The most frequently addressed concern was "Access permission", which was discussed in 18 out of 21 papers. There is great concern in ensuring that only authorized entities have access to patient data.

Ensuring access permission to authorized entities is essential to prevent theft or use of information without the patient's knowledge [28, 29] and to protect m-Health technology users from the Big Brother Effect [25].

This assurance can be obtained through the use of protocols and other mechanisms that guarantee to the

user that the access to their information is restricted [11]. As examples of solutions that reduce the threat of improper access, we can highlight the following: audit logs and log-off after a certain period of use [35]; continuous authentication, considering that the device can be used by others after the first access [16]; the use of cryptographic keys [25]; user authentication on the device for physical control unlocking and unauthorized access identification [21] or even solutions that leave the responsibility of the decision to the user, based on his/her preferences about who will gain access to his/her collected data [2, 31].

The second most frequently covered type of threat by authors was "Improper Information disclosure" (14 of 21 papers), relating to the user's loss of control over their information transmitted on m-Health technology [28]: the user's location, the type of sensor and information about their health conditions [30].

Secure data transmission is a factor that prevents incorrect disclosure of information. There are health regulation [11] guidelines on how this must be done [30]. However, this threat may often be related to an incorrect user choice, making it essential that m-Health solutions be designed to provide personalized user controls to ensure that the right information is being released to the right entities [11, 33].

The personalization of whats is shared, therefore, presents itself as a solution to avoid information disclosure [2, 16, 32]. Other solutions have been presented for this purpose, such as the use of cryptography [25], data anonymization, multi-factor authentication, notifications, audit logs [35, 21] and even contracts established between the patient, healthcare professionals and service providers that define how the data will be disclosed, respecting the patient's privacy preferences [31].

Undue disclosure of information has a direct impact on the adoption of these technologies, since users are strongly resistant to using them because they are afraid their data could be used by criminals [26] or for secondary purposes (commercial or marketing) [38]. However, m-Health users are willing to consent to the use of their data for medical research purposes [38].

Concerns about improper information disclosure are also related to the privacy personalization paradox: while the user needs to disclose his / her personal information and preferences to enjoy the personalized mobile health service, that user resists disclosing or revealing the minimum of information [37, 32]. The work that addressed this paradox identifies that trust is directly related to user concerns about privacy [37]. Trust mediates the effects of privacy concerns and perceived personalization and has different effects among different age groups [32].

Although approached by only 5 articles, "Device compromised, lost or stolen" is a privacy risk [35] that can lead to a person with malicious intent changing the data or resetting the patient's device [11], in addition to gaining access to information about the sensors used by the user, as well as their medical condition [30]. One of the major concerns of users is that their data can be stolen by hackers [28].

However, the risk of device loss, theft or compromise can be mitigated by using appropriate encryption and transmission protocols [11], difficult passwords, remote data deletion and device notifications [35]. Remote access in case of loss or theft is a necessary function to discard information, avoiding inappropriate use by third parties [21].

The "anonymity loss" threat, addressed by 4 of the 21 articles, is a factor that must be considered to have significant influence in the dissemination of information, especially when the user of the technology is under treatment of diseases that bear social stigmas [33], such as HIV. The data circulating in m-Health technology should be anonymous and the user should decide when to disclose them [11].

Among the solutions presented to guarantee the anonymity of users, we can highlight anonymization [35] and data transformation [16].

Although addressed in only 3 articles, "Service provider reliability" is essential, since many users are afraid that outsourced service providers will share their health data without consent [26]. In this respect, it is essential that technology providers (especially "in the Cloud") have tactics to convince the users to trust the service provided [35]. The solution to reduce this threat is to establish a contract that standardizes privacy treatment by providers, seeking to minimize the variations among the many service providers [31].

Finally, the risk of disclosure about device presence, present only in the work of [11], is related to the presence of the device as something private to maintain the patient's discretion. There are situations where you do not want other people to know that you are undergoing a certain type of treatment (using m-Health technology). For example, in the treatment of diseases that bear social stigma.

4.2. User privacy demands (SQ2)

This axis relates to human factors that can directly influence the use and adoption of m-Health technologies. When classifying the papers in this axis, we sought to identify which privacy demands, from the point of view of the users.

Table 3 shows that users' desire and willingness to share their health information were the demands with higher incidence in the selected papers, which indicates great fear and concern by users regarding the risks of privacy breach when sharing health information with third parties [35, 28]. Therefore, privacy has a direct influence on users' desire to share information on m-Health technology [28], since data sharing raises the question of consent: how and when does the person decide whether, and with whom, to share what data and at what level of granularity? [16]

Table 3. Distribution and percentage of articles by users' privacy demands. In some papers, more than one user demand was identified, so total is greater than 100%

User privacy demands	Related papers	%
Desire and willingness to share information	[24] [37] [16] [2] [26] [27] [28] [34] [39] [36][38] [35] [32][29] [33]	71.4
Privacy management	[37] [16] [38] [29] [31] [36][21] [40] [11][33] [35]	52.4
Information sharing perception	[2] [26] [35] [33] [11][31]	28.6
Privacy assurance mechanisms	[24] [38] [34] [26] [32] [36] [40] [31] [11][33] [35]	52.38
HCI (Human-Computer Interaction) usability issues	[25] [35] [30] [11]	19

Users' desire and willingness for sharing health information are directly associated with who will have access and for what purpose [24]. Health professionals involved in the treatment are singled out as the main target audience regarding users' interest in sharing their health information [27]. However, there is willingness to share information with other actors, but at different degrees and in a personalized way [2].

Among the main purposes that impact on the desire to share information is the individual's health situation [29, 36, 33, 34], directly influenced by certain factors such as type of problem experienced [33, 34], stage of the disease or if it bear some social stigma [29].

In the context of m-Health, conflicts of interest may arise between patients, hospitals and even service providers in relation to the dissemination of information [24]. In these cases, the patient should be considered the negotiator in the resolution of existing conflicts [36].

When designing an m-Health solution, it is critical that privacy and security aspects be considered [28]. Mechanisms must be created to ensure the privacy of m-Health technology. This is considered a user privacy demand, and is present in 11 of the 25 selected works. Among the proposed mechanisms, we emphasize privacy policies [11, 36, 34, 38, 24]. These mechanisms should be used so that there are no conflicts of interest between the patient and third parties and if they exist, they should be dealt with.

The research of Perez et. al [26] proposed dividing the mechanisms into two groups: those that allow data collection and those that do not. In the first group, the objective would be to create rules for data collection only in situations where users wish to divulge their information. In the second group, one approach would be a virtual wall that would allow users to define contexts where data collection should not be carried out.

Other mechanisms considered in the articles were laws, regulations [35] and access personalization [35, 31, 32], in other words, user control and authorization for a person to be entitled to receive their health information [31]. Customization mechanisms are resources for privacy management.

Privacy management, addressed in 11 of 21 articles, is the possibility for the user to customize the information to be shared in the context of m-Health [37, 16, 38, 35, 33]. As the disclosure of information depends on the patient's wishes, providing user controls is critical to ensure privacy [11, 21].

One solution that stands out among those presented for privacy management in m-Health is to allow the user to add / remove authorized entities (family, friends...) to receive or modify the view of their information mainly due to the different stages of a particular disease / treatment [40, 29]. In addition to these the adoption of privacy policies and the establishment of contracts between the user and the m-Health service provider [36] were also mentioned.

Another very important issue within the context of m-Health is the perception of how the user's Information is shared, since indirectly collected information is a major cause of non-acceptance of m-Health, as users are not always notified about disclosure of their data [2]. This aspect was mentioned in 6 of the 21 selected articles. In order for the user to be aware of any handling of operation on his / her data, m-Health technology should always notify them when the information is disclosed [11, 35] and who is using it [11, 26].

Due to large amounts of information being collected when using m-Health systems, it can be difficult for users to decide what information to share, and these choices can have important health consequences, so the right interface in each setting is important [11]. In this respect, HCI usability issues demonstrate the

user demand for user-friendly privacy and security systems [11, 35]. It is essential to develop simple and intuitive privacy protection mechanisms, involving and encouraging the user to handle such resources, regardless of the device used [35]. Although usability has been mentioned in only two articles, these issues are considered a challenge in designing m-Health with privacy and security in mind [11].

4.3. Contexts that impact users' privacy preferences (SQ3)

This axis tried to identify if the researches considered contexts that impact users' privacy preferences in the discussions or in m-Health technologies used as a reference.

Table 4. Distribution and percentage of articles addressing contexts that impact users' privacy preferences

Contexts	Related papers	%
Age	[2] [32]	9.5
Disease	[34] [29] [33]	14.2
Social factors	[2] [38] [27] [36]	19
Work environment	[2]	4.7
Does not address	[24] [37] [16] [25] [28] [35] [30] [21] [40] [11] [33] [31][26] [39]	57

Table 4 shows that m-Health technology users' privacy preferences are not static, they can change over time motivated by various factors or contexts.

Interest and willingness to share health information differed when comparing different age groups [2]. "Age" is a strong factor that directly affects privacy preferences [32].

Another context that impacts a patient's privacy preferences is Diseases. Concerns about patient privacy increase in the presence of certain types of disease that bear social stigma, leading the users to be more or less conservative in sharing their health information. [34, 29, 33]. The stage of a disease is also a factor that causes a change in the user's privacy preferences [29].

There are a variety of contexts that make the users feel the need to change their privacy preferences linked to social factors. There is a strong concern about sharing health information with family members so that they are not worried. With friends, the user is more willing to share health information [2, 38, 36]. The patients also reported that they do not believe that there is a social motivation in sharing health data with people with similar health conditions [27].

In the context related to work environment or profession, the motivator causing the user to change his / her privacy preferences is not related to the transparency of the information, but its use. The concern is with being adversely affected professionally because of their health condition [2].

Several studies mention that there are contexts that impact user privacy preferences, but they do not address or treat this more specifically and in-depth [31]. In Table 4, we can observe that more than half of the papers do not approach the subject; the remaining papers, although they do treat some specific contexts, are not concerned about analyzing other contexts that are not in their research. Privacy issues are a very important factor for the success of m-Health technology, these contexts that impact or can change user privacy preferences cannot be left out of the study, but what is observed is that this issue is not properly addressed in the researches.

4.4. Health domains (SQ4)

The health domains mentioned in the studies can be categorized under "Prevention", where the objective is to prevent the occurrence of any disease and "Management", where the objective is the treatment of disease. It can be observed that although prevention is included in the Table 5, studies that deal only with prevention issues were not identified. It is important to mention this because prevention is as important as management and requires attention.

Management is considered when the solutions also cover pre and post treatment [27] or when the disease is already controlled [28]. Treatment of chronic diseases is also considered management [29]. Dementia is an example of a chronic disease that requires monitoring [25]. In general, this domain is linked to patient monitoring [40]. Other work can be categorized in any other domains.

Table 5. Distribution and percentage of articles by health domains.

Health domains	Related papers	%
Prevention	-	0
Management	[25] [27] [28] [29] [40]	24
Any domain	[24] [37] [24] [16] [38][34] [26] [35] [21] [31] [32] [39] [36] [11] [33] [2]	76

4.5. Proposed solutions (SQ5)

Analyzing the results, we see a greater number of critical analysis, which indicate an exploratory nature of the m-Health privacy researches from a user's perspective. We consider critical analysis from more reflective research, which discusses privacy issues in

m-Health [29], often pointing to possible solutions [16, 2, 34, 26] to surveys, that seek to understand specific points of privacy, such as impact on the adoption/acceptance of m-Health technology [39, 33] or the impact of privacy on user behavior and intention to share information [37, 32].

Table 6. Distribution and percentage of article by solution presented. In some papers, more than one solution was identified, so total is greater than 100%

Solution presented	Related papers	%
Critical analysis	[16] [2] [34] [26] [33] [37], [28] [32] [29] [39]	42.9
Architecture	[25]	4.8
Method	[24]	4.8
Framework	[30], [21], [31], [36] [35] [11][28]	33.3
Recommendation	[2], [38], [27], [11]	19
State of art the review	[11]	4.8
Information System	[35], [36], [40], [33]	19

The second major contribution of the articles was in developing models, whether conceptual [11, 21], taxonomy - considering attributes of m-Health applications with respect to usability, security, and privacy [30], models that define rules of access/disclosure of information based on user profile [35, 31] and models to resolve conflicts between heterogeneous privacy policies and user-sharing preferences [36].

Other proposed solutions, albeit less frequently, have brought important contributions such as state of the art review, from an extensive literature review [11] and design recommendations for guiding m-Health device and application developers to build flexible privacy controls [2] and to reduce divisions (adoption/non-adoption) in a mHealth context [38]. These recommendations were obtained, in some cases, from interviews with health professionals and patients [27].

Some researchers developed information systems to implement the proposed models [35, 36]. Bachhal and Sandhu [40], however, create a remote patient health alert system that allows physicians to regularly update family and friends about elderly patient health conditions. Khorakhun and Bhatti [33], in turn, developed a self-monitoring application prototype to examine whether participants are more likely to share their data with professionals than with activity partners.

4.6. Target audiences (SQ6)

Since the concept of privacy is directly related to individual perception, it is important to know which target audience is considered in researches.

Table 7 shows that the majority of researches have no specific target, approaching generic m-Health users/patients. In some cases, the studies can also consider other actors involved in care or with the responsibility of handling health information. An example is a study by Sadki et al. [24], which addresses conflicts of privacy between privacy policies (from service providers, hospitals, researchers) and patients' desire for privacy.

Table 7. Distribution and percentage of articles by target audience. In some papers, more than one audience was identified, so total is greater than 100%

Target audience	Related papers	%
Generic (users and patients in general)	[24] [37] [16] [2] [26] [35] [21] [31] [39] [36] [11] [33] [32] [34]	66.7
Seniors	[38] [32] [40]	14.3
Health professionals	[27] [35] [31] [40] [33]	23.8
Family and friends	[27] [31], [40]	14.3
Patients with chronic diseases	[25] [27] [28] [29]	19
Hospital managers	[24]	4.8
Researchers	[24]	4.8
Cloud service providers	[24] [34] [31] [36]	19
Healthcare application developers	[28] [35] [30]	14.3

Other groups, although not so frequently in the papers selected, were part of important discussions, solutions and insights, such as in the case of health professionals, often demanding information from the patient for use in pre-clinical analysis [33]; patients with chronic diseases - slow-onset and long-term diseases lasting throughout one's lifetime - such as diabetes [28, 29], dementia [25] or musculoskeletal disorders [27] and seniors - a population group that is growing in view of the high rates of aging population, who from a certain age require monitoring for certain activities, in order to enjoy an autonomous but safe routine [40].

Two articles about seniors showed different results with regard to seniors' privacy demands. Guo et al. [32] conclude that the elderly a group that is less concerned with privacy (though less prone to adopting m-Health technology). Fox et al. [38] found that is a distrustful

public with respect to privacy, which would impact the adoption of m-Health [38]. Such divergence may indicate a demand for more research on this public.

5. Conclusion

This paper aimed to understand the privacy aspects related to users' desires and preferences in adoption and share their health information in m-Health technologies. For this, a systematic literature review was conducted focusing on the research question: "*What are the main issues addressed and solutions presented by the Computer Science community in recent years (2012-2018) about the user's privacy in m-Health technologies from the user's perspective?*"

The SLR resulted in few studies related to the topic, with only 21 papers, which contributes to the findings of Aleisa and Renaud [41], when investigating privacy in the context of IoT: more studies on privacy involving technology users are needed.

The results presented in this review demonstrate that "access permission" and "improper Information disclosure" were the most frequent types of threats to privacy in the papers analyzed. Similarly, "desire and willingness to share information", "privacy management" and "assurance of privacy mechanisms" were the most investigated user privacy demands. These findings demonstrated a convergence between these two axis (threats and user demands).

In most of the researches analyzed, the health domains and target audience are directed generically. However, privacy is related to the individual's perception and depending on cultural aspects and other characteristics, such as age, health status, current context.

Although we have used a strict method of literature review in the identification, screening and analysis of papers, the classifications and definitions of comparative axes are subjective and dependent on our understanding.

Even with limitations, the authors believe that this research has the potential to achieve its goal, firstly contributing toward an overview of m-Health privacy research regarding users' desires and preferences in sharing their health information in m-Health technologies and secondly to other research, exposing the major attributes to be addressed regarding privacy from the user's point of view, serving as important influence factors for the adoption of mHealth technology by users. One example found in the research is the ability for users to customize their privacy preferences, resulting in their being less concerned about the privacy of their health information.

Furthermore, it is important to highlight as a research finding that users' privacy desires and preferences are dynamic, changing because of various contexts. With regard to contexts that change user privacy preferences, the results demonstrated a weakness in this aspect because more than half of the articles do not address this issue, and when it is mentioned, it is superficially treated in the analyzed papers. This calls for future research to examine these contexts in more details, as it is an important factor for the success of m-Health technology.

References

[1] Global Observatory for eHealth, "Global diffusion of ehealth: Making universal health coverage achievable," tech. rep., World Health Organization, Geneva, Switzerland, 2016.

[2] A. Prasad, J. Sorber, T. Stablein, D. Anthony, and D. Kotz, "Understanding sharing preferences and behavior for mHealth devices," in *WPES '12*, (New York, New York, USA), p. 117, ACM Press, 2012.

[3] A. Westin, *Privacy and Freedom*. 1967.

[4] V. J. d. S. Rodrigues, *Gerência de Privacidade para Aplicações Sensíveis ao Contexto em Redes Móveis*. Phd thesis, Pontifical Catholic University of Rio de Janeiro, 2006.

[5] M. J. Dupuis, R. E. Crossler, and B. Endicott-Popovsky, "Measuring the human factor in information security and privacy," in *2016 49th Hawaii International Conference on System Sciences (HICSS)*, pp. 3676–3685, IEEE, 2016.

[6] M. S. Ackerman and S. D. Mainwaring, "Privacy issues and human-computer interaction," *Computer*, vol. 27, no. 5, pp. 19–26, 2005.

[7] A. Acquisti, M. Sleeper, Y. Wang, S. Wilson, I. Adjerid, R. Balebako, L. Brandimarte, L. F. Cranor, S. Komanduri, P. G. Leon, N. Sadeh, and F. Schaub, "Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online," *ACM Computing Surveys*, vol. 50, pp. 1–41, aug 2017.

[8] B. M. Silva, J. J. P. C. Rodrigues, F. Canelo, I. C. Lopes, and L. Zhou, "A data encryption solution for mobile health apps in cooperation environments.," *Journal of medical Internet research*, vol. 15, p. e66, apr 2013.

[9] S. Sharma, K. Chen, and A. Sheth, "Towards Practical Privacy-Preserving Analytics for IoT and Cloud Based Healthcare Systems." 2018.

[10] N. Saleheen, S. Chakraborty, N. Ali, M. M. Rahman, S. M. Hossain, R. Bari, E. Buder, M. Srivastava, and S. Kumar, "mSieve: differential behavioral privacy in time series of mobile sensor data," in *UbiComp '16*, (New York, New York, USA), pp. 706–717, ACM Press, 2016.

[11] S. Avancha, A. Baxi, and D. Kotz, "Privacy in mobile technology for personal healthcare," *ACM Computing Surveys*, vol. 45, pp. 1–54, nov 2012.

[12] L. J. Hoffman, "Computers and Privacy : A Survey," vol. I, no. 2, p. 19, 1969.

[13] S. Barth and M. D. de Jong, "The privacy paradox Investigating discrepancies between expressed privacy concerns and actual online behavior A systematic literature review," *Telematics and Informatics*, vol. 34, pp. 1038–1058, nov 2017.

[14] P. A. Pavlou, "State of the information privacy literature: Where are we now and where should we go?," *MIS quarterly*, pp. 977–988, 2011.

[15] E. Aïmeur, "Personalisation and privacy issues in the age of exposure," in *Proceedings of the 26th Conference on User Modeling, Adaptation and Personalization*, pp. 375–376, ACM, 2018.

[16] D. Kotz, C. A. Gunter, S. Kumar, and J. P. Weiner, "Privacy and Security in Mobile Health: A Research Agenda," *Computer*, vol. 49, pp. 22–30, jun 2016.

[17] B. Kitchenham, "Procedures for performing systematic reviews," tech. rep., Keele University, Keele, UK, 2004.

[18] J. Agarkhed, S. Mundewadi, S. S. Patil, *et al.*, "Mobile health monitoring system using cloud computing," in *2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, pp. 1301–1305, IEEE, 2016.

[19] F. D. Guillén-Gámez, I. García-Magariño, J. Bravo-Agapito, R. Lacuesta, and J. Lloret, "A proposal to improve the authentication process in m-health environments," *IEEE Access*, vol. 5, pp. 22530–22544, 2017.

[20] M. Plachkinova, S. Andrés, and S. Chatterjee, "A taxonomy of mhealth apps–security and privacy concerns," in *2015 48th Hawaii International Conference on System Sciences*, pp. 3187–3196, IEEE, 2015.

[21] F. Els and L. Cilliers, "Improving the information security of personal electronic health records to protect a patient's health information," in *2017 Conference on Information Communication Technology and Society (ICTAS)*, pp. 1–6, IEEE, mar 2017.

[22] C. Wohlin, P. Runeson, M. Höst, M. C. Ohlsson, B. Regnell, and A. Wesslén, *Experimentation in software engineering*. Springer Science & Business Media, 2012.

[23] D. Moher, A. Liberati, J. Tetzlaff, D. G. Altman, and T. P. Group, "Preferred Reporting Items for Systematic Reviews and Meta-Analyses: The PRISMA Statement," *PLoS Medicine*, vol. 6, p. e1000097, jul 2009.

[24] S. Sadki and H. El Bakkali, "Resolving Conflicting Privacy Policies in M-health based on Prioritization," *Scalable Computing: Practice and Experience*, vol. 17, pp. 207–226, aug 2016.

[25] A. Solanas, A. Martinez-Balleste, P. A. Perez-Martinez, A. F. de la Pena, and J. Ramos, "m-Carer: Privacy-Aware Monitoring for People with Mild Cognitive Impairment and Dementia," *IEEE Journal on Selected Areas in Communications*, vol. 31, pp. 19–27, sep 2013.

[26] A. J. Perez and S. Zeadally, "Privacy issues and solutions for consumer wearables," *It Professional*, vol. 20, no. 4, pp. 46–56, 2018.

[27] H. Chandra, I. Oakley, and H. Silva, "Designing to support prescribed home exercises: understanding the needs of physiotherapy patients," in *NordiCHI '12*, (New York, New York, USA), pp. 607–616, ACM Press, 2012.

[28] A. Maniam, J. S. Dhillon, and N. Baghaei, "Determinants of Patients' Intention to Adopt Diabetes Self-Management Applications," in *CHINZ 2015*, (New York, New York, USA), pp. 43–50, ACM Press, 2015.

[29] A. A. O'Kane, H. M. Mentis, and E. Thereska, "Non-static nature of patient consent: shifting privacy perspectives in health information sharing," in *CSCW '13*, (New York, New York, USA), p. 553, ACM Press, 2013.

[30] N. Asaddok and M. Ghazali, "Exploring the usability, security and privacy taxonomy for mobile health applications," in *2017 International Conference on Research and Innovation in Information Systems (ICRIIS)*, pp. 1–6, IEEE, jul 2017.

[31] S. Sadki and H. E. Bakkali, "PPAMH: A novel privacy-preserving approach for mobile healthcare," in *The 9th International Conference for Internet Technology and Secured Transactions (ICITST-2014)*, pp. 209–214, IEEE, dec 2014.

[32] X. Guo, X. Zhang, and Y. Sun, "The privacypersonalization paradox in mHealth services acceptance of different age groups," *Electronic Commerce Research and Applications*, vol. 16, pp. 55–65, mar 2016.

[33] C. Khorakhun and S. N. Bhatti, "mHealth through quantified-self: A user study," in *2015 17th International Conference on E-health Networking, Application & Services (HealthCom)*, pp. 329–335, IEEE, oct 2015.

[34] B. Koffi, A. Yazdanmehr, and R. Mahapatra, "Mobile health privacy concerns-a systematic review," 2018.

[35] S. Sadki and H. E. Bakkali, "Enhancing privacy on Mobile Health: An integrated privacy module," in *2014 International Conference on Next Generation Networks and Services (NGNS)*, pp. 245–250, IEEE, may 2014.

[36] S. Sadki and H. El Bakkali, "An approach for privacy policies negotiation in mobile health-Cloud environments," in *2015 International Conference on Cloud Technologies and Applications (CloudTech)*, pp. 1–6, IEEE, jun 2015.

[37] X. Guo, Y. Sun, Z. Yan, and N. Wang, "Privacy-Personalization Paradox in Adoption of Mobile Health Service: The Mediating Role of Trust," *PACIS 2012 Proceedings*, jul 2012.

[38] G. Fox and R. Connolly, "Mobile health technology adoption across generations: Narrowing the digital divide," *Information Systems Journal*, 2018.

[39] Hui-Mei Hsu, "Does privacy threat matter in mobile health service? From health belief model perspective," in *20th Pacific Asia Conference on Information Systems, PACIS 2016;*, 2016.

[40] G. S. Bachhal and A. K. Sandhu, "Remote patient health alert system," in *APCHI '13*, (New York, New York, USA), pp. 167–173, ACM Press, 2013.

[41] N. Aleisa and K. Renaud, "Privacy of the Internet of Things: A Systematic Literature Review," *Hawaii International Conference on System Sciences 2017 (HICSS-50)*, jan 2017.