International Journal of Medical Informatics 141 (2020) 104229

Contents lists available at ScienceDirect

International Journal of Medical Informatics

journal homepage: www.elsevier.com/locate/ijmedinf

Towards a contextual theory of Mobile Health Data Protection (MHDP): A realist perspective

Javad Pool[a,*], Saeed Akhlaghpour[a], Farhad Fatehi[b,c]

[a] UQ Business School, The University of Queensland, Brisbane, Australia
[b] Centre for Online Health, The University of Queensland, Brisbane, Australia
[c] School of Advanced Technologies in Medicine, Tehran University of Medical Sciences, Tehran, Iran

ARTICLE INFO

Keywords:
Mobile health
Data protection
Data privacy
Cybersecurity
Information systems

ABSTRACT

Background: With the introduction of privacy regulations such as the California Consumer Privacy Act and the European Union General Data Protection Regulation (GDPR), effective data protection in mobile health (mHealth) is rapidly becoming a concern. However, we have a limited understanding of the contexts and mechanisms that affect the likelihood of failures and successes in mHealth data protection, and their subsequent impacts. In this review and theory development paper, we aim to address this critical knowledge gap.

Method: We conducted a systematic literature search using PubMed, Embase, and Scopus databases. To synthesize the evidence, we adopted a realist review approach and compiled the extracted information based on context-mechanism-outcome (CMO) configurations. Out of an initial set of 611 records, 19 articles met the eligibility criteria and were included.

Results: Our findings indicate that the failures and successes in data protection and their impacts (effective mHealth interventions, data protection awareness, and adoption/use of mHealth systems) depend contingently upon a number of contextual factors (systems, users, tasks, services, geographic elements) and causal mechanisms (unauthorized access, device theft, loss, and sharing, lack of cyber-hygiene, and data protection concerns for failures, and trust building activity, secure and law compliant platforms, and perceived data protection, for successes). We conceptualized the CMO configurations to provide explanations for the reported failures and successes in data protection.

Conclusion: For effective mHealth interventions, the dark side of system use (data breaches) must be mitigated and remediated. Our study offers a theoretical model that contextually explains how the mechanisms of success and failures work in mHealth.

1. Introduction

In the digital health era, traditional models of care delivery have been transformed thanks to information technology-enabled services and business models [1–3]. A prominent ecosystem for effective care delivery is mobile health (mHealth) [4,5]. Internet-connected mHealth devices provide ubiquitous access to care providers to obtain personal health data. Meanwhile, patients can easily share their health information and receive health advice [6]. However, adoption and effective use of mHealth is tempered by data protection concerns [7,8]. From the perspective of both patients and providers, failures in the protection of personal health data are highly controversial and consequential [2,9]. This concern also is reflected in the World Health Organization (WHO) reports on mHealth and digital intervention, which highlighted calls for actions, policy and legal attention to ensure effective data protection [10,11].

Researchers have also documented several cases in mHealth context where mobile app developers are not transparent about data protection and also introduce intentional or by-product risks to effective data protection [12]. Furthermore, technical assessments of mHealth apps have revealed that several supposedly secure apps in healthcare did not adequately protect patient data. For example, a recent study on data sharing of top-rated mHealth apps in four developed countries found that the majority of the included apps for analysis shared personal data with third parties, ranging from birthday and email to medical conditions, and symptoms [13]. A similar study on 79 certified clinical apps showed security vulnerabilities and breaches such as sending sensitive information without encryption and authorized access to user data [14].

Effective data protection in mHealth is a technical and social

* Corresponding author.
E-mail addresses: j.pool@uq.net.au (J. Pool), s.akhlaghpour@business.uq.edu.au (S. Akhlaghpour), f.fatehi@uq.edu.au (F. Fatehi).

https://doi.org/10.1016/j.ijmedinf.2020.104229
Received 23 April 2020; Received in revised form 9 June 2020; Accepted 3 July 2020
Available online 11 July 2020

phenomenon. Apart from technical elements such as a system's privacy and security safeguards, social elements such as patients' trust and clinicians' practices in using the system play important roles in mHealth data protection failure and success [15–17]. As evident in our literature review, there is a paucity of theories that address the context-specific social and technical aspects of mHealth data protection. To advance the knowledge in this highly important context and embarking on the realist review approach, we aim to provide a theoretical model of failures and successes in mHealth data protection that is grounded in emerging evidence. By applying this approach, we sought to answer the following overarching research questions:

1 In what circumstances (contexts and mechanisms) is mHealth data protection most likely to be failed or successful?
2 What are the potential outcomes of mHealth data protection failures or successes?

Answering these questions can enhance our understanding of health data protection and more importantly facilitates theorizing the phenomena of mHealth data protection. Thereby, we move toward theorizing the phenomena by unpacking the context-mechanism-outcome (CMO) relationships and explaining the impacts of mHealth data protection failures and successes.

The rest of this paper is organized as follows: First, we describe our methodological approach in conducting the realist review. Next, we demonstrate our results in two sections: study characteristics and main findings, followed by a discussion of the mechanisms and outcome in the mHealth context. Finally, the conclusions are presented.

2. Methods

As our research aimed to provide a contextualized explanation of failures and successes of mHealth data protection, we adopted a realist review approach. Particular assumptions that realist review has about the nature of reality and causation make this theory-driven approach different from other types of reviews [18,19]. In this perspective, causal associations are influenced by the setting and context [20].

In conducting this review, we followed systematic steps recommended by Templier and Paré [21] to generate a new contribution to knowledge. These steps begin with practices concerning the formulation of research questions and include providing a meaningful way of analyzing and synthesizing data. As a key part and analytical unit of the realist review, data synthesis is performed by adopting context-mechanism-outcome (CMO) configurations. If we do not consider the context, here mHealth, we do not fully understand user-situation interaction and how data protection mechanisms get translated into outcomes [22]. These configurations allowed us to enrich our finding by generating causative explanations pertaining to both intended and unintended outcomes (i.e., failures and successes) [23]. Also, the CMO helps us to summarize and integrate extracted information into a unified and meaningful picture, which is not isolated from the mHealth context [24,25]. Thus, these configurations align properly with the aim of our study.

2.1. Search strategy

We performed a systematic search in academic literature published from 2010 to March 2019to capture a recent trend and up-to-date picture of failures and successes in mHealth data protection. A combination of keywords relevant to the aim of our study was used to conduct a comprehensive search in the PubMed, Scopus, and Embase databases. Search query and the number of hits are shown in Appendix Table A1. We also conducted a manual search of the reference lists.

2.2. Study selection process

The results of electronic searches were exported to an EndNote library and the duplicates were removed. For reviewing abstracts and full-text articles, we first specified inclusion and exclusion criteria, i.e., language, publication date, source type, subject area, type of system, data, and participants (see Appendix Table A2 for more details). Based on the inclusion and exclusion criteria and guided by PRISMA steps (identification, screening, eligibility and included), we selected the final set of articles regarding the mobile health data protection failures and successes in the literature.

2.3. Realist-informed analysis

In a realist review, ideally, researchers seek potentially eligible theories from the literature which can provide explanations of the phenomena under study [26]. Methodologically, by applying the critical analysis of empirical evidence, the initial candidate theories will be supported, extended and refined while some theories would be rejected [27]. However, in some cases of realist reviews, a viable candidate theory cannot be identified, which in turn, a tentative theory from primary studies can be built [28]. As an ideal and initial step in realist analysis, we sought to find candidate theories. However, from our knowledge of information security literature, the phenomenon of mHealth data protection has not been theorized. Thus, we inductively built an initial theory that contextually explains success and failure in mHealth data protection.

For coding and analyzing contextual factors of the included studies, we use Template Analysis, which is a form of thematic analysis [29]. One of the philosophical positions of this approach is contextualism, seeking a plausible account of the setting of the study [30]. Furthermore, to go along the path of theorizing, we used techniques in line with the grounded theory approach for openly coding and systematically analyzing the core category of the included empirical cases. Using grounded theory in a literature review has been recommended as it has a capacity for theoretical development and assuring in-depth analysis [31]. Facilitated by the CMO configurations, this approach strengthened our finding. We synthesized the core mechanisms of success and failures in mHealth data protection and provided the contextual explanation around the outputs and impacts accordingly.

3. Results

Fig. 1 shows the selection process. Our electronic search returned a total of 606 records from three databases. Also, five more articles were identified through other sources (e.g., reference check), making the initial set of 611 identified records. After removing duplicates, we screened 460 records at the title/abstract level. Of these, 372 articles were excluded for various reasons, leaving 88 potentially eligible articles. We then obtained and inspected the full-text of the articles based on our inclusion and exclusion criteria. In this step, 19 publications met the eligibility criteria. Throughout this process, study selection and data extraction were performed by the first author. The materials of these stages were shared continuously through a research collaboration tool (AARNet CloudStor) with the other two co-authors to monitor and review the decisions. Multiple meetings were conducted to discuss and resolve any uncertainty in the review process (the study selection and data extraction). In the following section, we provide a descriptive analysis and realist synthesis in the form of CMO configurations.

3.1. Descriptive characteristics

Table 1 provides the characteristics and descriptive statistics of the included studies. Half of the included studies were published between 2013 and 2015 and a limited number of publications were during 2010–2012, counting 17 %. The studies on mHealth data protection

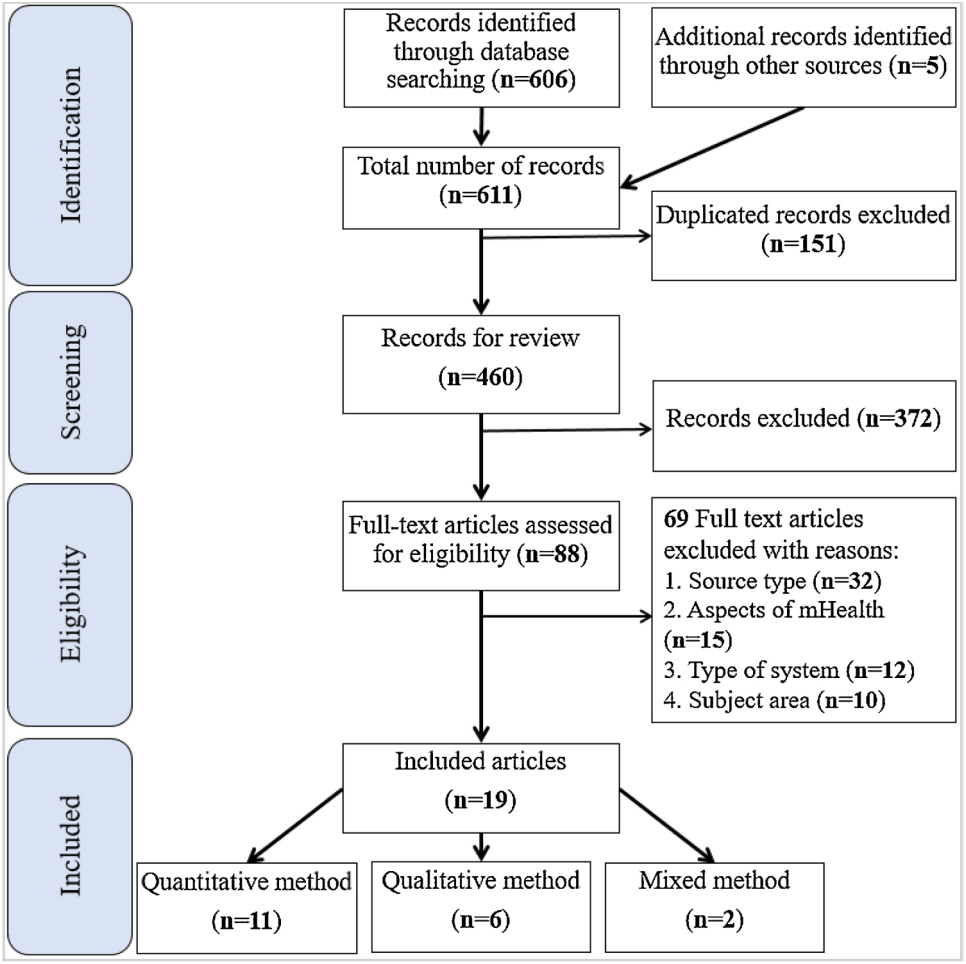

Fig. 1. PRISMA flowchart of study selection.

Table 1
Characteristics of the included articles.

Variable	Number of studies	Percentage
Year of publication		
2016–2019	7	37
2013–2015	9	47
2010–2012	3	16
Country		
North America (the USA and Canada)	5 (4,1)	26.3
Europe (UK, Ireland, Germany)	4 (2,1,1)	21.1
Asia (Singapore, Bangladesh, Philippines, Japan)	5 (2, 1,1, 1)	26.3
Africa (South Africa, Ghana, Kenya)	5 (3, 1, 1)	26.3
Economic Outlook (Based on IMF)		
Advanced economies	12	63
Emerging and developing economies	7	37
Systems		
Mobile phone	3	16
Smartphone	7	37
Mobile telehealth	2	10
Other portable mHealth devices (i.e., eye examination kit)	3	16
Multiple portable devices (i.e., mobile & wearable devices)	4	21
Method		
Quantitative	11	58
Qualitative	6	32
Mixed	2	10

were originated in various regions of the world. Unlike other reviews in information privacy and security where included studies were mainly conducted in the USA [32,33], in our review the studies took place in four regions, namely North America, Africa, Europe, and Asia with approximately similar percentages: 26.3 %, 26.3 %, 21.1 % and 26.1 %, respectively. Although the included publications were not dominated by USA-centric samples, 63 % of the studies originated from advanced economies, based on the country classification provided by *World Economic Outlook*. The information systems that the mHealth studies investigated were diverse, ranging from mobile phones to eye examination kit, of which the majority (37 %) refer to smartphones. In terms of methods, 11 articles used quantitative approaches while six articles applied qualitative inquiry and two articles conducted mHealth research by mixed methods (both quantitative and qualitative).

Only two articles (11 %) borrowed and tested theoretical frameworks particularly from information systems, the *Technology Acceptance Model (TAM)* and *Information System Success Model*.

A more detailed description of the included articles is shown in Appendix Table A3, covering authors, year of publication, title, journal, country, and methods.

3.2. Synthesis results

In this review, we put emphasis on mHealth data protection and argue that it should be understood as a complex phenomenon with substantial impacts in the context of healthcare eco-systems. To present a realist view of mHealth data protection failures and successes we have systematically analyzed and coded the content of the included articles,

Table 2
Grounded theory-informed coding.

1st Order Concepts	2nd Order Themes	Aggregate dimensions	Outcomes/Impacts	Representative examples
• Mobile phone accessed by others (family members and neighbors) • Reading mHealth text messages without the mobile owner's permission • Passcode identification by friends • Inappropriate method of notifications (medical test result) facilitated privacy violation • Providing incorrect phone numbers for receiving mHealth services • Failure to inform General Practitioners (GPs) when the contact details change	Unauthorized access	Failures	Effective mHealth intervention (i.e., management and follow-up of clients)	[35,36,37,16]
• A high rate of mobile theft • Phone theft in insecure remote areas	Device theft		Effective mHealth intervention (i.e., Clinic Appointment Reminders and Adherence Messages)	[35,36,38,39,17]
• Economic situation and unavailability of the phone for everybody facilitated cell phone sharing • SIM card sharing among rural users • Indirect use of system via taking health-related messages for other people • Sharing a cell phone with one or more other people	Device sharing		Effective mHealth intervention	[35,36,38]
• User unmindful action that causes the occurrence of mobile phone loss	Device loss		Effective mHealth intervention	[35,36,17]
• Not using data encryption and password protection to protect sensitive data • Using unsecured data storage (automatic cloud uploading systems and lack of control) • Keeping clinical images and patient forms on personal phone • Leave phones unattended and unsecured • Carrying phone on less secure parts (a handbag, backpack, or back pants pocket) • Unprotected data transmission • Lack of policy and standard for health data communication • Inappropriate way of communication with mHealth providers (i.e., e-mail)	Lack of cyber hygiene routine		Effective mHealth intervention	[16,39,17,40,41,15,42,43,44]
• Concerns about data protection and security of sensitive patient data • Concerns about personal data collection and data control, data processing, using, and sharing • *Lack of transparency* because of hidden agendas by service providers • Non-customized health promotion causes a privacy violation • Not obtaining specific consent from patients to text sensitive PHI	Matter of data protection concerns		Effective digital health intervention	[16,15,45,46]
• A secure medical data storage server • Systems characterized as a secure platform with an emphasis on trustworthiness, confidentiality, and privacy • Providing a secure and convenient manner for communication	Secure and law-compliant platform	Successes	Acceptance Satisfaction Raising awareness of the Data Protection Act (*through MyDoc as an educational tool*)	[47,48]
• Institutional endorsement of a health Intervention (e.g. university) • A strong relationship between users and providers • Getting permission for text messaging	Trust building activities		Effective mHealth intervention	[16,15]
• Patients not being of concerns (perceived) about providers for gaining access to their data • Perception of safety of wearable device connected with smartphones • Providing information for diabetic healthcare service from a remote place • Having the belief that providers do not share personal information with others • Perception of protection of personal data against loss or unauthorized access, destruction, modification, and disclosure. • Having the belief that providers do not disclose personal data without patients' authorization	Perceived data protection		Adoption of mHealth Effective mHealth intervention	[15,49]

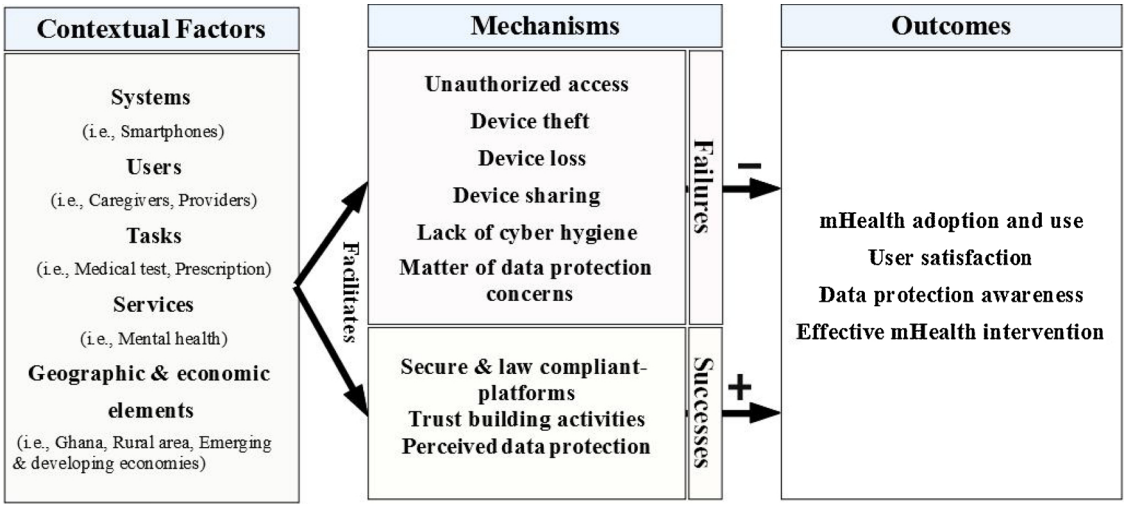

Fig. 2. A grounded theoretical model of mHealth data protection (MHDP).

Table 3
Definition of key mechanisms.

Key mechanism	Definition
Failure mechanism	One or multiple intentional/unaware actions that lead to, or increase, the likelihood of data breaches.
-unauthorized access	An abuse/misuse arising from an insider (e.g., a GP or a friend) who views and/or uses personal data
-device theft	The theft of smartphone, mobile phone and other portable devices used for mHealth.
-device loss	The loss of a smartphone, mobile phone and other portable devices used for mHealth.
-device sharing	A mindless action by a patient to share her/his devices (used for mHealth) with family or friends
-lack of cyber-hygiene routine	Not using cybersecurity related features (e.g., encryption, passcodes, secure clouds) of an mHealth system in the daily work and practices.
-data protection concerns	A patient's negative perception of data protection and data privacy regarding data processing by healthcare providers.
Success mechanism	One or multiple mindful actions that lead to, or increase, the likelihood of data protection.
-Secure and law-compliant platform	Using an mHealth system, which is secure, and in compliance with relevant regulations such as HIPAA or GDPR.
-Trust building activities	Actions (e.g., patient relationship management and obtaining consent) that increase patient trust and at the same time reduce patient concerns about unauthorized access.
-Perceived data protection	A patient's perception that her/his mHealth personal health data are protected by providers.

guided by Template Analysis and Grounded Theory methods.

In the coding process, we sought insights into the mechanisms of data protection failures and successes and how these mechanisms led into outcomes in the context of mHealth. We followed Gioia, Corley and Hamilton [34]'s approach for qualitative rigor and cycled between emergent concepts and themes from our synthesis and the relevant cybersecurity literature. The results of our grounded theory coding are presented in Table 2.

To demonstrate a theoretical model, we integrated the result of template analysis, contextual factors (see Appendix Table A4), and our grounded theory-informed coding. With this integrative approach, we were able to identify the patterns of failures and successes (see Appendix Table A5). A diagrammatic overview of the key results of the theoretical integration is provided in Fig. 2. Our approach conceptually formulates a grounded model of failures and successes in mHealth data protection. The model is emerged from a realist synthesis and is structured by CMO configurations. This theoretical model represents a subset of the phenomenon (mHealth data protection) in the real digital world [50]. In the following sections, we contextually explain and discuss the distinctive mechanisms that lead to the failures and successes, as well as the subsequent impacts.

3.3. An overview of key findings

As illustrated in Fig. 2, we organized the findings across four sections describing the contexts, key mechanisms of failures and successes, and their outcomes to explain the phenomenon of mHealth data protection. The nine key mechanisms emerged from our coding process were divided into two aggregate dimensions, failures and successes. Table 3 provides the detailed definitions of failures and successes mechanisms in our model.

Among the failure mechanisms, the first and most important is unauthorized access. This mechanism directly leads to data breaches and unintended consequences such as ineffective intervention [16,35–37]. There are also, other complex mechanisms including device sharing [35,38], loss and theft [17,36], lack of cyber-hygiene routine [2,15,39,42,43] and data protection concerns [15,45,46,51] that inhibit the process of adoption and effective use of mHealth [16,35,44,46]. On a separate block, mechanisms such as trust building activities [16], using secure and law compliant platforms [47,48], and perceived data protection [49] can result in positive outcomes such as user satisfaction and adoption of mHealth intervention [47,49].

4. Discussion

Our realist review revealed nine mechanisms as the fundamental drivers of mHealth data protection failures and success. In this section, we discuss the details of these key mechanisms and their outcomes. Building on a realist perspective, we demonstrate how mechanisms of mHealth data protection failure and success are invoked and consequently generate specific outcomes.

4.1. Failures in mHealth data protection

We define failures mechanisms in mHealth data protection as the mechanisms that lead to or facilitate personal health data breaches. In our study, these include 'unauthorized access', 'device theft', 'device loss', 'device sharing', 'lack of cyber-hygiene routine' and 'data

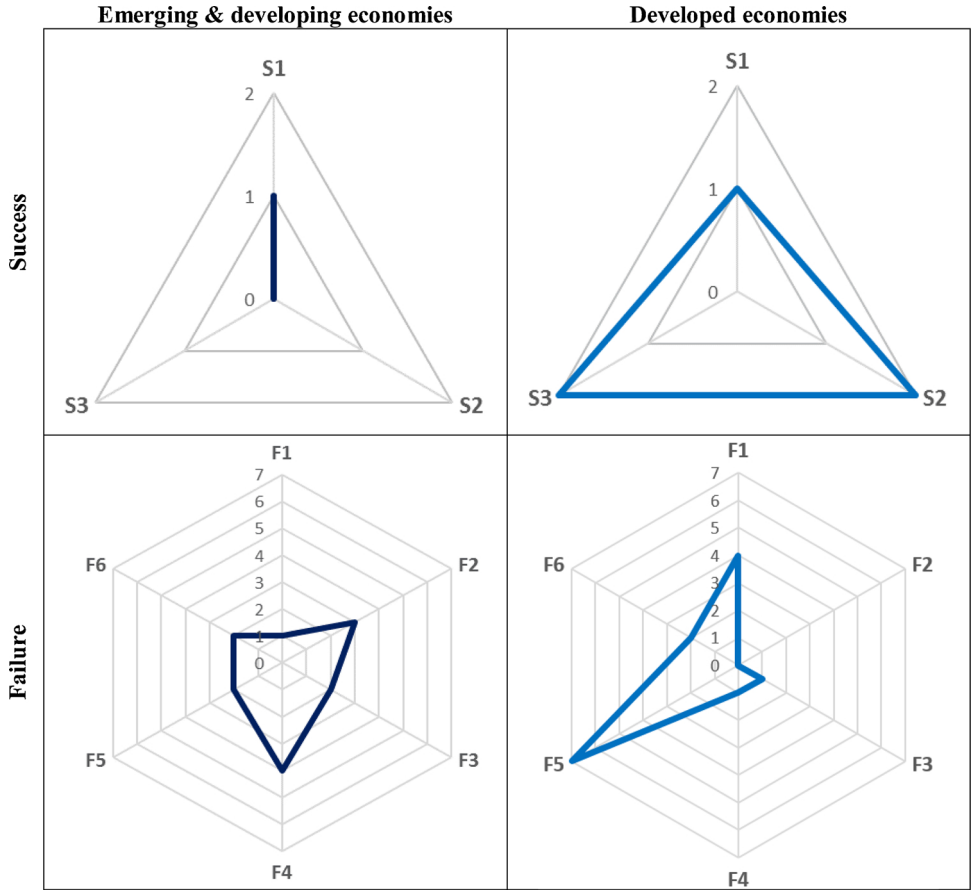

Fig. 3. Realist profiles of failure and success factors in mHealth data protection.

protection concerns' in various mHealth contexts.

'Unauthorized access' as the first failure mechanism represents a situation where a mobile phone is accessed by others, and upon that, an unauthorized person gains access to personal health data such as a clinical lab test result. This type of breach occurs in different contexts. As an example, in case of using mobile phones to improve health management (women eligible for a Pap smear, particularly HIV positive) in emerging and developing economies context (e.g., South Africa), a health care provider reported that their clients' mobile phones were accessed by others (family members and neighbors) when they were charging the battery [35]. In this case, one can read mHealth text messages without the mobile owner's permission. Similar to this incident, in case of appointment reminders and adherence messages in antiretroviral therapy clinic services, South African patients (25 % of respondents) believed that at some point their text messages had been read by an unauthorized person [36]. Furthermore, two instances of failure arose from a different context (advanced economies [Ireland]) related to the unauthorized access mechanism [16]. In one instance, some patients provided incorrect phone numbers for receiving mHealth services. In a second one, they failed to inform the service provider when they changed their phone numbers. These failures led to text messages being accessed by people other than the intended users. The outcome of the unauthorized access mechanism can restrict effective mHealth interventions. For example, embarrassment in a social setting and reluctance to use mHealth tools occurred as consequences of unauthorized access [16,37]. As the types of failure in different setting become increasingly diverse, it is important for care providers to use contextual best practices to minimize the risk of unauthorized access to ensure an effective mHealth intervention.

We identified three distinct failure mechanisms related to the use of the device, namely 'device theft', 'device loss', and 'device sharing'. Device theft and loss as the failures related to keeping personal devices safe were reported in a number of mHealth studies [17,38]. Among the studies that represent these types of failures, a significant percentage of participants reported experience in mobile phone loss or theft in the two studies in South Africa [35,36]. For example, 58 % of participants in a mHealth study conducted in Cape Town experienced theft or loss of mobile phones. Similarly, in an eye care study in Kenya, an issue related to data protection was that mobile phone users in insecure remote areas faced the risk of device theft [39]. Within the advanced economies context, one study (USA) in a mental health setting reported the failure in data protection raised from device theft/loss [17]. This study also reported that 24 % of psychologists and student trainees carrying their phone on less secure parts (e.g., a handbag, backpack, or back pants pocket) which could increase the likelihood of breaches. Another failure involving mHealth care is 'device sharing'. This mechanism of failure in our review only revealed in emerging and developing economies context, South Africa (see Fig. 3, F2) [35,36,38]. Further evidence of 'device sharing' mechanism is displayed in Appendix A6, where we summarized which mechanisms operate in which geographical and economic contexts. Care providers have expressed their concern of confidentiality of mHealth data that arise from this failure [35]. Overall, these three types of failure mechanisms, 'device theft', 'device loss', and 'device sharing', threaten the effectiveness and sustainability of mHealth interventions for the management and follow-up of clients [35,36].

As a central theme of our model of failures in mHealth data protection, 'Lack of cyber hygiene routine' was represented in nine studies (see Table 2). When users (providers and clients) neglect to effectively use or implement the security features of the system, other failures such as unauthorized access can arise. Not using data encryption and strong passwords to protect personal health data and secure communication

Table 4
Key practical implications from this study.

Practical implications (mechanisms in our model are highlighted in italics)	Proposed actions
General data protection - preventing data protection *failure mechanisms* and ensuring *successes mechanisms*	The model in this paper can be used as an assessment tool to identify failures and success in using mHealth technology. It can guide health data protection awareness programs on where (context) and how (mechanisms) failures can occur. This study suggests practitioners need to practice data-protection aware-use in mHealth data processing to build trust and increase adoption. It also recommends the development of mHealth-specific digital health intervention policies that protect health data and respect data subject rights such as the right to be informed.
Managing the risk of *unauthorized access*	Defining role base access to mHealth data by providers. Using a proper audit to evaluate that mHealth data accessed in authorized ways by health professionals and only used and processed for mHealth care delivery.
Managing the risk of *device theft, loss, and sharing*	Keeping of smartphone, mobile phone and other portable devices used for mHealth in a secure place. Using a tracking application to monitor device locations in case of device theft that will monitor device locations. Using the application with a feature that automatically deletes users' data/account if they are away for a period (e.g., one year), depending on the context. Adding secure passwords and multifactor authentication features to specific applications containing personal health data, in case of device sharing.
Establishing *cyber-hygiene routine* in practice to minimize the risk of *unauthorized access*	Storing clinical images only on providers' health systems. Defining an automatic lock (for short period) on mHealth devices. Transmitting and sharing health data only in an encrypted format. Developing and complying with information policy and standard for text messaging with patients Increasing health professionals' awareness and knowledge about a new type of cyber-attacks on mHealth systems where users (health professionals) are the main target for cyber-attacks (e.g., mobile phishing attacks).
Building *trust* with patients and reducing *data protection concerns*	Obtaining informed patient consent for using mHealth as a model of service delivery, and consent in terms of to whom their data can be shared and how the data will be used. Increasing transparency on how care providers used and shared mHealth data. Having mHealth data-breach-notification-plan for communicating with patients and trust recovery. Data minimization and restricting the future use of mHealth data by providers.
Managing the risk of *unauthorized access* by implementing a *secure and law-compliant platform*	Using mHealth systems that store health data in a region or country where patients reside (only use cross-border transfers where applicable privacy laws permit). Using mHealth systems that, by design and by default, required users to define strong passwords and are not automatically linked data to cloud storage. Not using third-party applications, which have not been approved by data protection authorities (e.g., using Facebook live for an mHealth consultation).

(e.g. patient images in plastic surgery) can result in the issue of non-compliance with data protection acts (e.g. HIPAA) and consequently facilitate cyber-crimes [40,41]. The key point emerged from our analysis was that the lack of cyber hygiene was not limited to the use of technical security features. The failures varied and involved users' insecure practices and lack of organizational security policies for communication. For example, patients used improper channels of communication with healthcare providers via their mobile phones. A study on the use of technology in mental health revealed that a patient, instead of using a provider platform, found and used his/her psychologist email for health-related communications. The user, then, sent an unencrypted email to the psychologist [43]. This type of action raises cybersecurity risks, stemmed from the clients. Lack of policy and standard for health data communication is another failure related to cyber hygiene routine. This failure was illustrated in a study of using mHealth in general practice [16]. For instance, the majority of GPs (76 %) reported not having a written security policy for text-messaging. The lack of cyber hygiene acts as a barrier for effective mHealth intervention since it can facilitate other failures such as unauthorized access and device theft or loss [17,35]. For mitigating this risk, restricting the use of mobile devices in the healthcare context can not be considered an effective strategy. For example, a study on the use of smartphones by nurses in the Philippines showed that such a restriction can lead to ineffective communication for service delivery [52]. Instead of imposing bans on the use of personal mobile devices, healthcare providers should design and implement an information security policy that supports and enhances cyber hygiene routines.

The final failure mechanism in our results was 'data protection concern'. This mechanism was mainly reported in studies from advanced economies such as the UK, Germany, and Ireland [15,16,45] with one exception from emerging and developing economy, Ghana [46].Data protection concerns are important for effective mHealth intervention as they impact the adoption and use of technologies. A study on the acceptance and use of mobile technology in a German medical center showed that both patients and physicians were worried about personal health data protection [45]. Patients also expressed their concern regarding the use of mobile devices for storing and processing health data. This concern could influence the effective use of mHealth. For example, 22.3 % of participants of the study indicated that they did not want their personal data saved or processed on a mobile device by health care providers. Another concern voiced by patients was about the lack of transparency. In a perspective analysis of early psychosis service users on digital technology, results showed that participants preferred the interventions endorsed by doctors rather than by health organizations [15]. Hidden agenda by care providers in data processing is an important reason why users exhibit resistance towards digital interventions. A different data protection concern was reported in a study in Ghana with a focus on receiving health promotion via text messages for noncommunicable diseases [46]. In this study, contextualized in community pharmacies for expanding access to the screening of noncommunicable diseases, 39.4 % of participants raised concern regarding receiving unsolicited mHealth messages as a violation of privacy. The result of the aforementioned cases, in early psychosis service and noncommunicable diseases, highlight that health organizations also need to focus on the social endorsement practices, i.e., transparent data processing and customized services, to reduce data protection concerns.

4.2. Successes in mHealth data protection

We define mHealth data protection success mechanisms as the mechanisms that enhance the protection of personal health data and emphasize patients' rights to data privacy. Three success mechanisms emerged from our analysis, namely, 'secure and law-compliant platform', 'trust building activities', and 'perceived data protection', which were, in turn, influential in achieving mHealth success.

Using a 'secure and law-compliant platform' as the first success mechanism refers to use of secure mHealth systems, which is approved by or fitted with data protection acts (e.g. HIPAA or GDPR), for healthcare delivery. In our review, MyDoc was presented as an illustrative example of an mHealth platform that was secure and aligned with the Personal Data Protection Act (PDPA) of Singapore in the orthopedic surgery setting [47]. This mHealth platform was characterized by a secure medical data storage server, ensuring trustworthiness, confidentiality, and privacy, and facilitating regulatory-compliant communication [47,48]. Raising awareness of the PDPA through using MyDoc as an educational tool in orthopedics setting was indicated as a successful outcome [47]. In the same context, user satisfaction was also mentioned as an outcome of this successful system [47,48].

'Trust building activities' is the second mechanism of success in our model. We identified two concepts related to this mechanism in the advanced economies context, institutional endorsement of a health intervention (e.g. by a university) and getting permission for text messaging [15,16]. As an example in the psychosis service, legitimized organizations (respected mental health charity) and a strong relationship between users and providers as a trust building activity can increase customer confidence about information security in health intervention [15]. Another aspect of trust building activities was "privacy by design and default". For instance, in a study on text messaging in general practice, GPs indicated that consent for text messaging were embedded by design in the practice management systems and registration. If patients did not consent to receiving mHealth services, GPs were not allowed to provide the clinical services via text messaging [16]. Thus, trust building activities regarding the personal health data at both institutional and individual levels are important. Health care organizations (e.g. data protection officers monitoring the integrity and availability of digital health assets) and employees (e.g. GPs involved in mHealth data processing) must act in such a way that does not undermine the patients' perception of data protection and trustworthiness. Activities that undermine trust, as discussed in the failure mechanisms, threatens the legitimacy of care providers. Also, they can affect patients' perception in a way that their data is not effectively protected and consequently cause ineffective mHealth intervention.

The final mechanism of success in our model is 'perceived data protection'. This mechanism refers to the perception of the users that their personal health data are protected by care providers. The positive perception of data protection is an important element in our model as it has an impact on the adoption of mHealth and effectiveness of interventions [15,49]. When customers perceive that their personal health data is protected against loss or unauthorized access, destruction, modification, and disclosure, they are more likely to adopt mHealth solutions. This outcome of data protection is supported by an investigation into mobile health adoption behavior in a Bangladeshi diabetes care setting [49].

4.3. Practical implications

In this study, we focused on mHealth systems. The mechanisms that we identified pertain to mHealth systems and are different from the other domains of digital health. These differences arise from certain features of mHealth such as portability and multi-functionality (work and personal use). For example, theft of desktop computers in a hospital setting is quite unlikely compared to the theft of portable devices such as smartphones. Also, in comparison to other digital health technologies such as Electronic Medical Records (EMR), mHealth systems and devices are widely used by both patients and health professionals. Generally, mobile technologies are used for multiple proposes and can contain personal data, organizational data, and health data. Furthermore, mechanisms such as device sharing and device loss are distinct in mHealth context. Finally, practices such as cyber-hygiene routines are highly dependent on the context. As a comparison, data protection practices related to the use of blockchain technologies in healthcare are predominantly technical and pertinent to organizational level actors. Data protection failures stemming from the design, decentralized storage, or data integrity can be the main concerns in the use of blockchain in health care [53,54]. These concerns are fundamentally different in the context of mHealth use.

The existing privacy regulations such as the GDPR, HIPAA, and/or local country-specific laws provide the overarching guiding principles for data protection. However, they are inherently broad and applicable to different contexts. Given the importance and idiosyncrasies of the mHealth data protection context, we used a realist review approach to identify context-specific practices and generate actionable advice. This approach is consistent with the recurrent calls to "*to take the context into greater consideration to generate insights about the phenomena associated with information technologies (IT), individuals, and organizations*" [55, p.112]. Apart from the contextualized model developed in this paper, Table 4 illustrates a number of practical implications of our findings that can inform data protection policies and practices.

5. Conclusion

mHealth systems are designed to support caregivers and healthcare organizations, and enable patients to receive high-quality health services. It is important to use the system in a way that increases medical task performance. However, with neglecting data protection aspects, success in health service excellence simply cannot be achieved. To make an effective mHealth intervention, the dark side of system use (data breaches) must be mitigated and remediated. This requires an understanding of the contexts and generative mechanisms that result in mHealth data protection-aware use. Drawing on a realist review, our study demonstrates a theoretical model that contextually explains how the mechanisms of failure and success lead to different outcomes in mHealth settings. The findings of this study can offer a novel perspective on data protection and contribute to more informed decisions for the development of effective mHealth interventions. Kurt Lewin [56, p.118], widely regarded as one of the founding fathers of social psychology famously stated, "there's nothing so practical as good theory". We aspire that our realist review and attempt towards developing a contextualized theory of mHealth data protection can be an enabler of effective data protection in practice.

Summary points

What was already known on the topic:

- Mobile health (mHealth) is a promising area of digital health transformation.
- Lack of data protection in mHealth context is a mounting concern for users.
- Data privacy and security issues in mHealth are barriers to the adoption and use.
- Our understanding of contexts and mechanisms that result in failure or success in mHealth data protection in practice is limited.

What this study adds to our knowledge:

- This study reports on a realist review for identifying the contexts and mechanisms that affect the likelihood of failures and successes in mHealth data protection, and their subsequent impacts.
- It proposes a theoretical model for explanations of failures and successes in mHealth data protection.

- It describes how complex mechanisms such as unauthorized access and lack of cyber-hygiene can challenge the effective use of mHealth and digital health interventions.
- Similarly, it elaborates on trust building activities and using law compliant platforms by providers as important mechanisms of mHealth data protection.

;1;

Authors' contributions

JP, SA and FF conceptualized and designed the study. JP conducted the literature search and reviewed the identified records based on inclusion/exclusion criteria. JP synthesized the included articles and formulated the initial theoretical model. JP and SA developed the final model. JP wrote a first draft of the manuscript with intellectual input from SA and FF. All authors contributed to the final version.

Declaration of Competing Interest

The authors have no competing interests to declare.

Appendix A

Table A1
Search queries and number of hits for each database.

Search #	Databases	Query**	Hits
1	PubMed	("Data protection" OR "Data breach*" OR "Security breach*" OR "Privacy breach*" OR "Security incident*" OR "unauthorized access" OR "unauthorised access" OR Theft OR Security attack* OR Cybersecurity OR Cyber security OR Cyber-security OR Privacy invasion OR Privacy violation*) ***AND*** (mHealth OR "Mobile Health" OR "mobile phone*" OR "cell phone*" OR Messenger OR Messag* OR tablet* OR apps OR smartphone* OR "smart phone*" OR "personal digital assistant*" OR portable OR iPad OR iPhone)	133
2	Embase	#1	169
3	Scopus	#1 AND (health OR medic* OR patient*)	304
Total			606

**: In the title, abstract or keywords; and Publication date to 2019/03/24.

Table A2
Details of Study Selection Criteria (Inclusion/Exclusion).

	Inclusion Criteria	Exclusion Criteria
Language	English	Other than English
Text availability	Full text	Full text not available
Publication dates	2010-2019/03/24	Before 2010 and After 2019/03/24
Source type	Journal (original /research articles), peer review	Review, opinion; perspective, view, letter, comment and response, conference paper, Symposium proceedings paper
Subject area	Failures and successes in mobile health data protection Impacts of failures and successes	Not relevant to the failures and successes in mobile health data protection and impacts
Type of system	mHealth (mobile phone, Smartphones, apps for health and wellbeing, Instant Messaging Apps in Healthcare, personal digital assistants (PDA) phones, portable devices capable of recording, storing and/transferring health data (e.g. Google glass))	Not related to mHealth systems, mHealth systems lacking the capability for data processing such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination (Based on GDPR)
Aspects of mHealth studies	Social and technical (consistent with IS theorization, we considered articles investigating both sides)	Studies that solely focus on the technical aspect of mHealth (e.g. system architecture, algorithms), and neglecting to place the social aspect of mHealth use (e.g. patient behaviour, capabilities, and user experience)
Data	Electronic, Personally identifiable information (PII)	Non-electronic
Participants	mHealth users, care providers related to mHealth services	Individuals not involving in data processing or not relevant to the data subject

Table A3
General descriptions of the included articles.

Author/s	Year	Title	Journal	**Country**	**Method**
Moodley, Constant, Botha, van der Merwe, Edwards and Momberg [35]	2019	Exploring the feasibility of using mobile phones to improve the management of clients with cervical cancer precursor lesions	BMC Women's Health	South Africa	Mixed method
Lam, Simpson and Lau [41]	2019	Health Insurance Portability and Accountability Act Noncompliance in Patient Photograph Management in Plastic Surgery	Annals of Plastic Surgery	USA	Quantitative
Guo, Phan, Ho, Pawlovich and Kitson [40]	2018	Clinical texting among medical trainees of the university of British Columbia	Journal of Cutaneous Medicine and Surgery	Canada	Quantitative
Bucci, Morris, Berry, Berry, Haddock, Barrowclough, Lewis and Edge [15]	2018	Early psychosis service user views on digital technology: qualitative analysis	JMIR mental health	UK	Qualitative
Akutey, Der, Owusu-Daaku and Baiden [46]	2018	Using community pharmacies to expand access to screening for noncommunicable diseases in suburban Ghana—A facility-based survey on client needs and acceptability	Health Science Reports	Ghana	Quantitative
Leahy, Lyons, Dahm, Quinlan and Bradley [16]	2017	Use of text messaging in general practice: A mixed methods investigation on GPs' and patients' views	British Journal of General Practice	Ireland	Mixed method
Lodhia, Karanja, Lees and Bastawrous [39]	2016	Acceptability, Usability, and Views on Deployment of Peek, a Mobile Phone mHealth Intervention for Eye Care in Kenya: Qualitative Study	JMIR Mhealth Uhealth	Kenya	Qualitative
Bautista and Lin [44]	2016	Sociotechnical analysis of nurses' use of personal mobile phones at work	International Journal of Medical Informatics	Philippines	Qualitative
Daruwalla, Loh and Dong [47]	2016	Spaced Education and the Importance of Raising Awareness of the Personal Data Protection Act: A Medical Student Population-Based Study	JMIR medical education	Singapore	Quantitative
Elhai and Hall [17]	2015	How secure is mental health providers' electronic patient communication? An empirical investigation	Professional Psychology: Research and Practice	USA	Quantitative
Gkatzidou, Hone, Sutcliffe, Gibbs, Sadiq, Szczepura, Sonnenberg and Estcourt [37]	2015	User interface design for mobile-based sexual health interventions for young people: design recommendations from a qualitative study on an online Chlamydia clinical care pathway	BMC medical informatics and decision making	UK	Qualitative
Muensterer, Lacher, Zoeller, Bronstein and Kübler [42]	2014	Google Glass in pediatric surgery: An exploratory study	International journal of surgery	USA	Quantitative
Jack and Mars [38]	2014	Ethical considerations of mobile phone use by patients in KwaZulu-Natal: Obstacles for mHealth?	African journal of primary health care & family medicine	South Africa	Quantitative
Illiger et al. [45]	2014	Mobile technologies: expectancy, usage, and acceptance of clinical staff and patients at a university medical center	JMIR Mhealth Uhealth	Germany	Quantitative
Daruwalla et al. [48]	2014	The application of telemedicine in orthopedic surgery in singapore: a pilot study on a secure, mobile telehealth application and messaging platform	JMIR Mhealth Uhealth	Singapore	Quantitative
Shareef et al. [49]	2014	Predicting mobile health adoption behaviour: A demand side perspective	Journal of Customer Behaviour	Bangladesh	Quantitative
Okazaki et al. [51]	2012	Factors affecting mobile diabetes monitoring adoption among physicians: questionnaire study and path model	Journal of Medical Internet research	Japan	Quantitative
Van Allen and Roberts [43]	2011	Critical Incidents in the Marriage of Psychology and Technology: A Discussion of Potential Ethical Issues in Practice, Education, and Policy	Professional Psychology: Research and Practice	USA	Qualitative
Crankshaw et al. [36]	2010	Exploring the patterns of use and the feasibility of using cellular phones for clinic appointment reminders and adherence messages in an antiretroviral treatment clinic, Durban, South Africa	AIDS patient care and STDs	South Africa	Qualitative

Table A4
Template coding.

Study	The geographic and economic element	Type of disease/health issue	Setting/organization/ service provider	User	System	Task
1. Moodley, Constant, Botha, van der Merwe, Edwards and Momberg [35]	Emerging and Developing Economies (EDE), South Africa	Cervical cancer precursor lesions	Public sector health services	Women eligible for a Pap smear, particularly HIV positive clients	Mobile Phone	Communication (test result and appointment reminders)
2. Lam, Simpson and Lau [41]	USA, Advanced Economies (AE)	Not Applicable (NA)	Accreditation Council for Graduate Medical Education (Plastic surgery programs)	Members of the American Society of Plastic Surgery and trainees	Smartphone and use of application: SMS, iMessage, Facebook messenger, and Whatsapp	Capturing patient photographs
3. Guo, Phan, Ho, Pawlovich and Kitson [40]	Canada, AE, Services for rural and remote British Columbia	NA	University, dermatology services	Medical trainees (medical students, residents, and fellow) in both rural and urban settings	Smartphone	Communication (text messages and attached clinical photos in medical practice)
4. Bucci, Morris, Berry, Berry, Haddock, Barrowclough, Lewis and Edge [15]	UK, AE	Mental health, Psychosis	Psychosis service	Early psychosis service users	Smartphone	Communication (symptom monitoring and self-management support)
5. Akutey, Der, Owusu-Daaku and Baiden [46]	Ghana, EDE	Noncommunicable diseases	Community pharmacies	Clients for noncommunicable diseases (NCDs) screening	Smartphone	Communication (receiving NCD promotion through text messages)
6. Leahy, Lyons, Dahm, Quinlan and Bradley [16]	Ireland, AE	N/A	General practice service	GPs and patients	Mobile phone AND web-based text messages	Communication (GPs: communicating with patients, and patients: receiving text messages from their GP)
7. Lodhia, Karanja, Lees and Bastawrous [39]	Kenya, EDE	Eye-related issue	Eye Care	Patients and health care providers	The Portable Eye Examination Kit (Peek)	eye (ophthalmic) testing
8. Bautista and Lin [44]	Philippines, EDE	N/A	Hospital	Nurses	Personal mobile phones (Smartphone: 96 %)	Communication (nurse-to-physicians, -patients and their relative), documentation
9. Daruwalla, Loh and Dong [47]	Singapore, AE	N/A	National University of Singapore	Medical students in orthopedics	Mobile telehealth application and messaging platform (MyDoc)	Communication (student-to-student and student-to-doctor)
10. Elhai and Hall [17]	USA, AE	N/A	Cognitive-behavioural psychotherapy	Psychologists and student trainees ("Female clinicians were more likely to password-protect their phones")	Smartphone	Communication (with patients by exchanging email and text messages)
11. Gkatzidou, Hone, Sutcliffe, Gibbs, Sadiq, Szczepura, Sonnenberg and Estcourt [37]	UK, AE	Sexually transmitted infections (Chlamydia)	Higher education institution, and Education College/ online sexual clinical care	young people (16–24) from colleges and higher education "Security was not perceived as a major potential barrier as participants were generally unaware of potential security threats and inherently trusted new technology" "Occasionally participants became frustrated when they were asked to disclose certain information about sexual history information"	Smartphone	Communication (test result and prescription and asking questions)
12. Muensterer, Lacher, Zoeller, Bronstein and Kübler [42]	USA, AE	N/A	Pediatric surgery	A *researcher* as a user of Google Glass, and response from colleagues, staff, families and patients	Google Glass	Telementoring (video recording and transmission)
13. Jack and Mars [38]	South Africa, *Urban and remote* rural area, EDE, "Rural respondents were significantly more likely to share SIM cards with other people"	Not specified (N/S), General	Private (fee-for-service medical care) and government-funded hospitals	Patients attending practitioners and outpatient	Mobile phone	Communication (Contacting the hospital and doctor for advice or medical reminders)

(*continued on next page*)

Table A4 (*continued*)

Study	The geographic and economic element	Type of disease/health issue	Setting/organization/ service provider	User	System	Task
14. Illiger, Hupka, von Jan, Wichelhaus and Albrecht [45]	Germany, AE	N/S	University hospital	Doctors and patients "Patients are more critical of the devices being used for storing and processing patient data"	Mobile devices (smartphone and/or a tablet PC)	Patients' health-related activities (finding a diagnosis, managing fitness) and communication with physicians
15. Daruwalla, Wong and Thambiah [48]	Singapore, AE	N/A	University Hospital, orthopedic surgery	Doctors, program director, program coordinator, one trauma consultant, all orthopedic residents, and six non-orthopedic residents	Mobile telehealth application and messaging platform (MyDoc)	Communication (personal messages, announcements for residents, case discussions, providing patient details for referrals, and showing a photo of a radiograph being taken to upload on the system for a referral)
16. Shareef, Kumar and Kumar [49]	Bangladesh, EDE	Diabetes	Diabetes care	Patients with diabetes	Wearable (hospital-provided) device and Smartphone	Diabetes management (diabetes check-ups and monitoring activity and diet level and calories) and Communication (diabetes consultancy and SMS for regular instructions and tips)
17. Okazaki, Castañeda, Sanz and Henseler [51]	Japan, AE	Diabetes	Diabetes care	Physicians specialized in general internal and gastrointestinal medicine	Mobile diabetes monitoring	Monitoring (control of blood glucose, weight, physical activity, diet, insulin and medication, and blood pressure)
18. Van Allen and Roberts [43]	USA, AE	N/A	Psychology	Psychologists	Smartphone	Communication (Psychologists -to-patient)
19. Crankshaw, Corless, Giddy, Nicholas, Eichbaum and Butler [36]	South Africa, EDE	Activity of retroviruses: HIV-related health infection	Antiretroviral therapy (ART) clinic	ART patients "Phone Sharing was significantly greater for females compared to males"	Mobile phone	Communication (appointment reminders and adherence messages)

Table A5
A representative example of Context-Mechanism-Outcome (CMO) analysis.

	Context						Outcomes
	Geographic/economic element	*Type of disease/ health issue*	*Setting/organization/ service provider*	*User*	*System*	*Task*	
Study 1: Moodley, Constant, Botha, van der Merwe, Edwards and Momberg [35]	Emerging and Developing Economies (EDE), South Africa	Cervical cancer precursor lesions	Public sector	Women eligible for a Pap smear, particularly HIV positive clients	Mobile Phone	Test result and appointment reminders	Management and follow-up of clients, Success and sustainability of mHealth intervention
	Theft or loss of mobile phones: "high rate of mobile phone loss or theft (58%)" ***Mobile phone sharing***: "Many patients are not working and cannot afford a cell phone, and not everybody owns a cell phone" ***Unauthorized access***: "Leaving mobile phone to charge the battery and someone picks it up and reads SMS (a family member or a neighbor)" **Mechanism of failures (data breaches)**						

Table A6
The geographic and economic contexts and the related mechanisms.

Country	Region	Economic Outlook	Mechanism		Reference
			Failure	Success	
South Africa	Africa	Emerging and Developing Economies	Unauthorized access, Device theft, *Device sharing*, Device loss	×	Moodley et al. (2019)
			Device theft, *Device sharing*	×	Jack and Mars (2014)
			Unauthorized access, Device theft, *Device sharing*, Device loss	×	Crankshaw et al. (2010)
Ghana			Data protection concerns	×	Akutey et al. (2018)
Kenya			Device theft, Lack of cyber hygiene routine	×	Lodhia et al. (2016)
Bangladesh	Asia	Emerging and Developing Economies	×	Perceived data protection	Shareef et al. (2014)
Philippines			Lack of cyber hygiene routine	×	Bautista and Lin (2016)
Singapore	Asia	Advanced Economies	×	Secure and law-compliant platform	Daruwalla et al. (2016)
			×	Secure and law-compliant platform	Daruwalla et al. (2014)
Japan			Data protection concerns (failure of the perception of the severity of data breach)	×	Okazaki et al. (2012)
USA	North America	Advanced Economies	Lack of cyber hygiene routine	×	Lam et al. (2019)
			Device theft, Device loss, Lack of cyber hygiene routine,	×	Elhai and Hall (2015)
			Lack of cyber hygiene routine	×	Muensterer et al. (2014)
			Lack of cyber hygiene routine	×	Van Allen and Roberts (2011)
Canada			Lack of cyber hygiene routine	×	Guo et al. (2018)
UK	Europe	Advanced Economies	Unauthorized access	×	Gkatzidou et al. (2015)
			Lack of cyber hygiene routine, Data protection concerns	Trust building activities, Perceived data protection	Bucci et al. (2018)
Ireland			Unauthorized access, Lack of cyber hygiene routine, Data protection concerns	Trust building activities	Leahy et al. (2017)
Germany			Data protection concerns	×	Illiger et al. (2014)

References

[1] M. Herrmann, P. Boehme, T. Mondritzki, J.P. Ehlers, S. Kavadias, H. Truebel, Digital transformation and disruption of the health care sector: internet-based observational study, J. Med. Internet Res. 20 (2018) e104.
[2] R. Agarwal, G. Gao, C. DesRoches, A.K. Jha, Research commentary—The digital transformation of healthcare: current status and the road ahead, Inf. Syst. Res. 21 (2010) 796–809.
[3] E. Karahanna, A. Chen, Q.B. Liu, C. Serrano, Capitalizing on health information technology to enable digital advantage in US hospitals, MIS Q. 43 (2019) 113–140.
[4] D. Kauw, M.A.C. Koole, M.M. Winter, D.A.J. Dohmen, I.I. Tulevski, S. Blok, G.A. Somsen, M.P. Schijven, J.W.J. Vriend, D. Robbers-Visser, B.J.M. Mulder, B.J. Bouma, M.J. Schuuring, Advantages of mobile health in the management of adult patients with congenital heart disease, Int. J. Med. Inform. 132 (2019) 1–6.
[5] A. Roess, The Promise, Growth, and reality of mobile health — Another data-free zone, N. Engl. J. Med. 377 (2017) 2010–2011.
[6] L. Chen, A. Baird, A. Rai, Mobile health (mHealth) channel preference: an integrated perspective of approach-avoidance beliefs and regulatory focus, J. Assoc. Inf. Syst. 20 (2019) 1743–1773.
[7] M.-P. Gagnon, P. Ngangue, J. Payne-Gagnon, M. Desmartis, m-Health adoption by healthcare professionals: a systematic review, J. Am. Med. Inform. Assoc. 23 (2015) 212–220.
[8] I. Sim, Mobile devices and health, N. Engl. J. Med. 381 (2019) 956–968.
[9] J. Kwon, M.E. Johnson, Proactive versus reactive security investments in the healthcare sector, MIS Q. 38 (2014).
[10] WHO, mHealth: New Horizons for Health Through Mobile Technologies, Global Observatory for eHealth Series, Geneva, Switzerland, 2011.
[11] WHO, WHO Guideline: Recommendations on Digital Interventions for Health System Strengthening, World Health Organization, Geneva, 2019, pp. 1–46.
[12] A. Sunyaev, T. Dehling, P.L. Taylor, K.D. Mandl, Availability and quality of mobile health app privacy policies, J. Am. Med. Inform. Assoc. 22 (2014) e28–e33.
[13] Q. Grundy, K. Chiu, F. Held, A. Continella, L. Bero, R. Holz, Data sharing practices of medicines related apps and the mobile ecosystem: traffic, content, and network analysis, BMJ 364 (2019) l920.
[14] K. Huckvale, J.T. Prieto, M. Tilney, P.-J. Benghozi, J. Car, Unaddressed privacy risks in accredited health and wellness apps: a cross-sectional systematic assessment, BMC Med. 13 (2015) 214.
[15] S. Bucci, R. Morris, K. Berry, N. Berry, G. Haddock, C. Barrowclough, S. Lewis, D. Edge, Early psychosis service user views on digital technology: qualitative analysis, JMIR Ment. Health 5 (2018) e10091.
[16] D. Leahy, A. Lyons, M. Dahm, D. Quinlan, C. Bradley, Use of text messaging in general practice: a mixed methods investigation on GPs' and patients' views, Br. J. Gen. Pract. 67 (2017) e744–e750.
[17] J.D. Elhai, B.J. Hall, How secure is mental health providers' electronic patient communication? An empirical investigation, Prof. Psychol. Res. Pract. 46 (2015) 444–450.
[18] R. Pawson, The Science of Evaluation: a Realist Manifesto, Sage, London, 2013.
[19] J. Durham, V. Nanhthavong, V. Sychareun, Explaining how unexploded ordnance clearance enhances livelihoods in the Lao PDR, Eval. Program Plann. 54 (2016) 82–93.
[20] S.M. Dalkin, J. Greenhalgh, D. Jones, B. Cunningham, M. Lhussier, What's in a mechanism? Development of a key concept in realist evaluation, Implement. Sci. 10 (2015) 49.
[21] M. Templier, G. Paré, A framework for guiding and evaluating literature reviews, Commun. Assoc. Inf. Syst. 37 (2015) 6.
[22] G. Johns, The essential impact of context on organizational behavior, Acad. Manage. Rev. 31 (2006) 386–408.
[23] S.R. Kirsh, D.C. Aron, K.D. Johnson, L.E. Santurri, L.D. Stevenson, K.R. Jones, J. Jagosh, A realist review of shared medical appointments: how, for whom, and under what circumstances do they work? BMC Health Serv. Res. 17 (2017) 113.
[24] H. Cooper, Research Synthesis and Meta-Analysis: a Step-by-Step Approach, Sage publications, 2015.
[25] L. Dubé, G. Paré, Rigor in information systems positivist case research: current practices, trends, and recommendations, MIS Q. (2003) 597–636.
[26] G. Wong, T. Greenhalgh, R. Pawson, Internet-based medical education: a realist review of what works, for whom and in what circumstances, BMC Med. Educ. 10 (2010) 12.
[27] J. Jagosh, Realist synthesis for public health: building an ontologically deep understanding of how programs work, for whom, and in which contexts, Annu. Rev. Public Health 40 (2019) 361–372.
[28] T. Greenhalgh, F. Macfarlane, L. Steed, R. Walton, What works for whom in pharmacist-led smoking cessation support: realist review, BMC Med. 14 (2016) 209.
[29] J. Brooks, S. McCluskey, E. Turley, N. King, The utility of template analysis in qualitative psychology research, Qual. Res. Psychol. 12 (2015) 202–222.
[30] N. King, J. Brooks, S. Tabari, Template Analysis in Business and Management Research, Qualitative Methodologies in Organization Studies, Springer, 2018, pp. 179–206.
[31] J.F. Wolfswinkel, E. Furtmueller, C.P. Wilderom, Using grounded theory as a method for rigorously reviewing literature, Eur. J. Inf. Syst. 22 (2013) 45–55.
[32] F. Bélanger, R.E. Crossler, Privacy in the digital age: a review of information privacy research in information systems, Mis Q. 35 (2011) 1017–1042.
[33] N. Shen, T. Bernier, L. Sequeira, J. Strauss, M. Silver, A. Carter-Langford, D. Wiljer, Understanding patient privacy perspective on health information exchange: a systematic, Int. J. Med. Inform. (2019).
[34] D.A. Gioia, K.G. Corley, A.L. Hamilton, Seeking qualitative rigor in inductive research: notes on the Gioia methodology, Organ. Res. Methods 16 (2013) 15–31.
[35] J. Moodley, D. Constant, M.H. Botha, F.H. van der Merwe, A. Edwards, M. Momberg, Exploring the feasibility of using mobile phones to improve the management of clients with cervical cancer precursor lesions, BMC Womens Health 19 (2019) 2.
[36] T. Crankshaw, I.B. Corless, J. Giddy, P.K. Nicholas, Q. Eichbaum, L.M. Butler, Exploring the patterns of use and the feasibility of using cellular phones for clinic appointment reminders and adherence messages in an antiretroviral treatment clinic, Durban, South Africa, AIDS Patient Care STDS 24 (2010) 729–734.
[37] V. Gkatzidou, K. Hone, L. Sutcliffe, J. Gibbs, S.T. Sadiq, A. Szczepura, P. Sonnenberg, C. Estcourt, User interface design for mobile-based sexual health interventions for young people: design recommendations from a qualitative study on an online Chlamydia clinical care pathway, BMC Med. Inform. Decis. Mak. 15 (2015) 72.
[38] C.L. Jack, M. Mars, Ethical considerations of mobile phone use by patients in KwaZulu-Natal: obstacles for mHealth? Afr. J. Prim. Health Care Fam. Med. 6 (2014) E1–E7.
[39] V. Lodhia, S. Karanja, S. Lees, A. Bastawrous, Acceptability, usability, and views on deployment of peek, a mobile phone mhealth intervention for eye care in Kenya: qualitative study, JMIR Mhealth Uhealth 4 (2016) e30.
[40] D. Guo, N. Phan, K. Ho, J. Pawlovich, N. Kitson, Clinical texting among medical trainees of the university of british columbia, J. Cutan. Med. Surg. 22 (2018) 384–389.
[41] J.S. Lam, B.K. Simpson, F.H. Lau, Health insurance portability and accountability act noncompliance in patient photograph management in plastic surgery, Ann. Plast. Surg. (2019).
[42] O.J. Muensterer, M. Lacher, C. Zoeller, M. Bronstein, J. Kübler, Google glass in pediatric surgery: an exploratory study, Int. J. Surg. 12 (2014) 281–289.
[43] J. Van Allen, M.C. Roberts, Critical incidents in the marriage of psychology and technology: a discussion of potential ethical issues in practice, education, and policy, Prof. Psychol. Res. Pract. 42 (2011) 433–439.
[44] J.R. Bautista, T.T. Lin, Sociotechnical analysis of nurses' use of personal mobile phones at work, Int. J. Med. Inform. 95 (2016) 71–80.
[45] K. Illiger, M. Hupka, U. von Jan, D. Wichelhaus, U.V. Albrecht, Mobile technologies: expectancy, usage, and acceptance of clinical staff and patients at a university medical center, JMIR Mhealth Uhealth 2 (2014) e42.
[46] R. Akutey, R. Der, F. Owusu-Daaku, F. Baiden, Using community pharmacies to expand access to screening for noncommunicable diseases in suburban Ghana-a facility-based survey on client needs and acceptability, Health Sci Rep 1 (2018) e79.
[47] Z.J. Daruwalla, J.L. Loh, C. Dong, Spaced education and the importance of raising awareness of the personal data protection act: a medical student population-based study, JMIR Med. Educ. 2 (2016) e12.
[48] Z.J. Daruwalla, K.L. Wong, J. Thambiah, The application of telemedicine in orthopedic surgery in singapore: a pilot study on a secure, mobile telehealth application and messaging platform, JMIR Mhealth Uhealth 2 (2014) e28.
[49] M.A. Shareef, V. Kumar, U. Kumar, Predicting mobile health adoption behaviour: a demand side perspective, J. Cust. Behav. 13 (2014) 187–205.
[50] R. Weber, Evaluating and developing theories in the information systems discipline, J. Assoc. Inf. Syst. 13 (2012) 1–30.
[51] S. Okazaki, J.A. Castañeda, S. Sanz, J. Henseler, Factors affecting mobile diabetes monitoring adoption among physicians: questionnaire study and path model, J. Med. Internet Res. 14 (2012) e183.
[52] J.R. Bautista, T.T. Lin, Y.-L. Theng, Influence of organizational issues on nurse administrators' support to staff nurses' use of smartphones for work purposes in the Philippines: focus group study, JMIR Nurs. 3 (2020) e17040.
[53] T. Hardin, D. Kotz, Blockchain in health data systems: a survey, 2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS), IEEE, 2019, pp. 490–497.
[54] T. McGhin, K.-K.R. Choo, C.Z. Liu, D. He, Blockchain in healthcare applications: research challenges and opportunities, J. Netw. Comput. Appl. (2019).
[55] W. Hong, F.K. Chan, J.Y. Thong, L.C. Chasalow, G. Dhillon, A framework and guidelines for context-specific theorizing in information systems research, Inf. Syst. Res. 25 (2014) 111–136.
[56] K. Lewin, Psychology and the process of group living, J. Soc. Psychol. 17 (1943) 113–131.