Journal of Public Health: From Theory to Practice
https://doi.org/10.1007/s10389-021-01608-9

ORIGINAL ARTICLE

A new privacy framework for the management of chronic diseases via mHealth in a post-Covid-19 world

Farad Rafique Jusob[1] · Carlisle George[1] · Glenford Mapp[1]

Received: 8 October 2020 / Accepted: 21 May 2021

Abstract

Aim New challenges are being faced by global healthcare systems such as an increase in the elderly population, budget cuts as well as the ongoing Covid-19 pandemic. As pressures mount on healthcare systems to provide treatment to patients, mHealth is seen as one of the possible solutions to addressing these challenges. Given the sensitivity of health data, the rapid development of the mHealth sector raises privacy concerns. The aims of this research were to investigate privacy threats/concerns in the context of mHealth and the management of chronic diseases and to propose a novel privacy framework to address these concerns.

Subject and method The study adopted a modified version of the engineering design process. After defining the problem, information was gathered through literature reviews, and analyses of existing regulatory (privacy) frameworks and past research on privacy threats/concerns. Requirements for a new framework were then specified leading to its development and comparison with existing frameworks.

Results A novel future-proof privacy framework was developed and illustrated. Using existing regulatory frameworks for privacy and privacy threats/concerns from research studies, privacy principles and their resulting requirements were identified. Furthermore, mechanisms and associated technologies needed to implement the privacy principles/requirements into a functional prototype were also identified. A comparison of the proposed framework with existing frameworks, showed that it addressed privacy threats/concerns in a more comprehensive manner.

Conclusion This research makes a valuable contribution to protecting privacy in mHealth. The novel framework developed is an improvement on existing frameworks. It is also future-proof since its foundations are built on regulatory frameworks and privacy threats/concerns existing at the time of its deployment/revision.

Keywords Privacy · mHealth · Self-management · Chronic diseases · Framework

Introduction

In March 2020, the World Health Organization declared the coronavirus outbreak as a pandemic, which is continuing at the time of writing. As a result of this pandemic, healthcare systems have been overwhelmed and stressed, resulting in various patients having their appointments cancelled and being told to stay home in order to limit the spread of the infectious disease. Owing to overcrowding in urgent care clinics, emergency departments and primary care clinics, the implementation of mHealth systems can be used as a solution to provide care to patients with chronic illnesses as well as reduce in-person clinic visits (Rockwell and Gilroy 2020).

The emergence and rapid development of mHealth has the potential to play an important role in the transformation of healthcare and increase its quality and efficiency. mHealth solutions cover various technological solutions that allow their users to measure vital signs such as heart rate, blood glucose level and blood pressure (European Commission 2014). Sensors and mobile applications are used to collect medical, physiological, lifestyle, daily activity and environmental data that could serve as a basis for evidence-driven care practice and research activities, while allowing patients access to their

✉ Farad Rafique Jusob
fj105@live.mdx.ac.uk

Carlisle George
c.george@mdx.ac.uk

Glenford Mapp
g.mapp@mdx.ac.uk

[1] School of Science and Technology, Middlesex University, London, UK

Published online: 18 June 2021

health information at any given time or place. mHealth can also support the delivery of high-quality healthcare and enable more accurate diagnosis and treatment. It can support healthcare professionals in treating patients more efficiently as mobile apps can encourage adherence to a healthy lifestyle, resulting in more personalised medication and treatment. It can also contribute to patient empowerment as they would be able to manage their health more actively whilst still living more independent lives in their own home environment due to self-assessment or remote monitoring solutions (European Commission 2014; Conroy 2015). mHealth enables a broad range of health-related applications to share data with health providers (as in a traditional doctor–patient relationship) and with insurance companies (Steinhubl, 2015).

According to the World Health Organization (2017), non-communicable diseases (NCD) or chronic diseases, such as diabetes and obesity, have been found to be one of the largest challenges to worldwide healthcare systems. These diseases were responsible for over 40 million global deaths each year. The use of mHealth systems such as mobile applications and wearable technologies can assist users with prevention of chronic diseases as well as improve the treatment prescribed to patients with chronic diseases based on their daily habits (Estrin and Sim 2010). According to Watkins et al. (2018) chronic diseases require consistent self-care and monitoring in order to examine their regression or progression as well as provide one- or two-way communication between practitioners and patients. A study carried out by Yi et al. (2018) concluded that out of 13 studies, 11 found that mHealth provided patients with a statistically beneficial effect.

Safeguarding personal data and addressing privacy concerns is an important aspect of mHealth. In the context of mHealth, managing privacy is a complex issue: patients need control over the collection, recording, dissemination and access to their mHealth data (Kotz et al. 2009). Generally, patients can regulate who has access to their personal health information through the giving of informed consent. Informed consent gives patients appropriate knowledge of what data are being collected, how they are stored and used, what rights they have to the data and what the potential risks of disclosure could be. However, technological literacy limits users' understanding of the true threats and advantages of technology. Because of users' limitations on technological literacy, it is necessary to develop mHealth systems that allow patients added control over their data such as, what data is collected and who has permission to access it (Arora et al. 2014).

This study focuses on investigating privacy concerns in mHealth especially in the context of managing chronic diseases. It also focuses on developing a solution to these privacy concerns by the development of a privacy framework for mHealth.

Methodological approach

The methodological approach adopted for this study is a modified version of the engineering design process (Khandani 2005), and consisted of the following processes:

Definition of the problem The problem was defined to identify and establish the need for a new privacy framework for mHealth in the context of monitoring chronic diseases.

Information gathering Review of relevant literature was carried out which focused primarily on (i) identification of privacy threats and concerns from previous research studies and (ii) an analysis/comparison of current regulatory frameworks for privacy.

Analyse, select and generate solution Framework requirements were specified after (i) an analysis of regulatory frameworks for privacy, to determine relevant privacy principles; (ii) a gap analysis was undertaken in order to identify and determine which privacy concerns and threats were addressed by existing regulatory frameworks for privacy; (iii) a framework was generated, implemented and evaluated.

mHealth and privacy problems

Although the use of mHealth supports and facilitates the provision of high-quality healthcare and enables more accurate diagnosis and treatment, numerous previous studies (some cited below) have shown that mHealth poses privacy threats and concerns. A study by Dehling et al. (2015) concluded that 95% of 17,979 mHealth apps surveyed posed some potential damage (information leaks, manipulation, loss, access by third parties) due to privacy and security infringements. A feasibility study on privacy risks of 298 mHealth apps by Brüggemann et al. (2016) found various privacy risks, including that 40% of 70 apps (where data transfer could be identified) transferred personal data without encryption. According to Hussain et al. (2018), mHealth apps are vulnerable to privacy threats which include identity theft, disclosure threats, leakage of information, storage of unencrypted data and the use of data by third parties. In a study by Hutton et al. (2018) assessing privacy in 64 mHealth apps, they found that the majority of the apps performed poorly on privacy, including not allowing users sufficient access to their data, not allowing sufficient control of the granularity of data shared and having inadequate consent mechanisms. Iwaya et al. (2019) carried out a privacy impact assessment of the GeoHealth system, a large-scale mHealth data collection system used in Brazil to deliver community care. They discovered 97 different privacy threats

relating to issues such as data quality, informed consent, legitimacy of processing, data security and accountability. They also classified these threats as 89% likely to happen and only 11% unlikely to happen.

In addition to studies on the actual privacy risks of mHealth systems, some studies have concluded that perceived privacy risks of mHealth services by patients make them less likely to trust and adopt mHealth services. Zhang et al. (2014) conducted a study consisting of 491 participants which concluded that privacy can indirectly influence mHealth adoption because privacy negatively impacted participants attitudes and perceived usefulness of mHealth. Guo et al. (2016) surveyed 650 subjects on mHealth services and concluded that privacy concerns had a negative association with trust and adoption of such services. In a study of 388 patients, Deng et al. (2018) concluded that trust correlated positively with patients' intention to adopt mHealth services, and that privacy risks correlated negatively with trust and hence adoption intention.

The studies cited above are a few examples demonstrating that privacy threats and concerns in mHealth services pose actual or perceived risks to patients, they violate commonly accepted privacy requirements/regulations (e.g. data security, informed consent, accountability) and impact negatively on the adoption of mHealth services. These privacy threats and concerns provide a rationale for further research into finding solutions to prevent or mitigate their consequences. The work carried out in this study is one such research project which focuses on proposing a solution, by developing a suitable privacy framework to better develop mHealth systems so that privacy threats and concerns can be more effectively addressed.

Privacy threats and concerns for mHealth when managing chronic diseases

A privacy concern is an emotional state that may leave someone distressed with regard to their personal information. On the other hand, a privacy threat is something that may or may not happen but has the ability to potentially cause harm to a patient (e.g. unlawful access to and use of a patient's personal information). It is important to implement safeguards to counteract privacy threats and ensure that patient privacy is preserved. However, it is also important to address privacy concerns in order for patients to have an improved sense of trust and confidence in mHealth systems.

Previous research studies have concluded that mHealth used in any context raises many privacy threats and concerns as described in Table 1. Table 1 lists the various processes that a typical user would undergo in order to monitor their chronic disease with the support of mHealth. Each process has different privacy threats and concerns associated which were gathered from various sources of literature. This is necessary in order to understand what users go through and to have a better understanding of the possible threats and concerns associated with the processes. It must be noted that there can be more than one threat associated with some processes.

Figure 1 illustrates various events in an mHealth scenario where data is processed (e.g. inputted, collected, transmitted, used). It also highlights the key areas that give rise to privacy threats and concerns (indicated by letters in circles).

The events as shown in Fig. 1 include: manual input of data from a patient (P); the collection of data from body sensors (C); the transmission of data between different stages (T); the

Table 1 Identification of privacy threats/concerns – mHealth and monitoring chronic diseases

Processes in mHealth monitoring	Privacy threat/concern
Data collection and activity monitoring using wearables or sensors	• Continuous monitoring (Avancha et al. 2012) • Volume of data collection (Steinhubl et al. 2015) • Invisibility (Brey 2005)
Communication between wearable device and mobile phone	• Data security (Steinhubl et al. 2015) • Encryption (Avancha et al. 2012) (Steinhubl et al. 2015) • Confidentiality (Harvey and Harvey 2014)
Location tracking using mobile phones	• Profiling (Avancha et al. 2012) • Surveillance (Shilton 2009)
Sharing of data with healthcare practitioners, insurance companies and other users	• Data use (unauthorised or unanticipated) (European Commission 2011) • Sharing of data (Avancha et al. 2012) • Information misuse/abuse (European Commission 2011)
Manual data input	• Data quality (Avancha et al. 2012)
Use of mobile applications	• Encryption (McCarthy 2013) • Data control (Arora et al. 2014) • Accessibility (Arora et al. 2014) • Disclosure risks (Steinhubl et al. 2015)
Doctor to patient communication	• Confidentiality (Harvey and Harvey 2014)

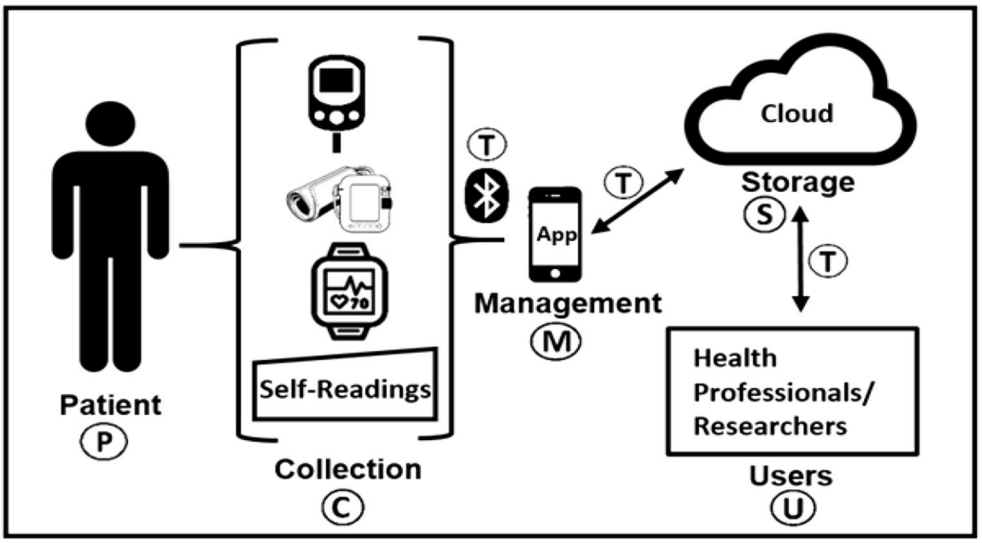

Fig. 1 Stages of processing mHealth Data

management of data on a smartphone app (M); the storage of data in the cloud (S); and the use of data by various types of users (U). The privacy concerns associated with each of the events are further discussed below.

Table 2 summarises the privacy concerns/threats at different events in an mHealth scenario.

Comparison of relevant existing regulatory frameworks for privacy

The authors conducted a previous study comparing relevant existing regulatory frameworks for privacy and how they address privacy concerns in mHealth (Jusob et al. 2017). These frameworks included: Health Privacy Project (HPP) Best Practice Principles of 2007 (Kotz et al. 2009); Markle Common Framework of 2008 (Markle Foundation 2008); Office of the National Coordinator for Health Information Technology (ONC) Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information of 2008 (ONC 2008); Generally Accepted Privacy Principles (GAPP) of 2008 (Prosch 2008); A Privacy Framework for Mobile Health and Home-Care Systems (MHHCS) of 2009 (Kotz et al. 2009); Organisation for Economic Co-operation and Development (OECD) Principles of 2013 (OECD 2013); General Data Protection Regulation (GDPR) (EC 2016).

The study identified at least 23 privacy principles collectively addressed by all frameworks namely: accountability; assignment of proxy; chain of trust; choice and consent; collection and data minimisation/limitation; correction (accurate data); data anonymisation and pseudo-anonymity; data

Table 2 Privacy threats/concerns at each stage of data processing

Privacy threats and concerns for mHealth and chronic diseases	Data processing events in mHealth					
	(P)	(C)	(M)	(T)	(S)	(U)
Accessibility of data			•		•	•
Anonymity			•		•	•
Confidentiality						•
Continuous monitoring		•				
Data control					•	•
Data quality	•	•				
Data security			•	•	•	
Data use (limitation)						•
Disclosure risks			•	•	•	•
Encryption			•	•		
Information misuse/abuse						•
Invisibility	•					
Profiling			•			
Sharing of data						•
Surveillance		•	•			
Volume of data collection		•				

management; data quality and integrity; education; enforcement and remedies; fair and lawful processing; individual access; individual choice; individual participation and control; medical sensing devices not made observable by other parties; notice; openness and transparency; portability; purpose specification of data collection; security safeguards and encryption; storage limitation; use limitation.

The study found that no single framework addressed all of the 23 privacy principles. The study also concluded that no existing privacy framework adequately addressed all privacy threats and concerns (identified in existing literature) when using mHealth to manage chronic diseases.

Proposing a new privacy framework for mHealth

Framework requirements

Based on an analysis of (i) existing regulatory frameworks for privacy and (ii) privacy threats and concerns identified in previous research, the following requirements were specified for a new framework.

- The new framework must be underpinned (i.e. have a fundamental base) by a body of literature on privacy obligations and guidelines of existing regulatory frameworks and the need to address privacy threats and concerns identified from previous research.
- The new framework should specify high level privacy principles to reflect the privacy obligations and guidelines of existing regulatory frameworks and the need to address privacy threats and concerns.
- The new framework should specify privacy requirements for each privacy principle in order to implement the principle into a functional software system.
- The new framework should specify what mechanisms and technologies are to be used to implement the privacy requirements derived from the privacy principles.
- The new framework should be capable of being implemented into a working software prototype.
- The new framework should be capable of being illustrated in a diagrammatic form.

Framework development

After the framework requirements were specified, several brainstorming activities (involving experimenting with various diagrams) were conducted to determine how best to illustrate the framework concept to meet the specifications. After several iterative attempts, a diagrammatic format was generated and selected to best represent how various specification requirements should be combined to create the new framework. A multi-layered structure was selected consisting of each layer building upon the previous layer. The contents of the base layer were selected to ensure that the framework could be implemented at any time in the present or future. In order to implement privacy principles, specific privacy requirements for a prototype needed to be developed using syntax based on the work of the Mitre Corporation (2015) and Raimundas (2017). Furthermore, the mechanisms and associated technologies to implement the privacy requirements were identified.

The proposed framework in this work is illustrated in Fig. 2 and attempts to comprehensively address known privacy obligations and threats/concerns in existing literature. It consists of five layers namely (1) regulatory frameworks for privacy and privacy threats and concerns (2) privacy principles, (3) privacy requirements, (4) mechanisms and associated technologies, and (5) prototype.

Framework layer 1 – regulatory frameworks for privacy + privacy threats and concerns This layer starts with (ii) identifying existing regulatory frameworks, together with (ii) identifying privacy threats and concerns based on existing research. These provide a future-proof applicability of the framework, since the framework will be based on regulatory frameworks and research existing at any point in time (current or future) when the framework is implemented. For this study, as discussed previously, relevant regulatory frameworks were identified and compared. Also, privacy threats and concerns when using mHealth in the context of monitoring chronic diseases were identified from existing research (see Table 1).

Framework layer 2 – privacy framework principles This layer outlines the various privacy principles that are developed from an analysis of the information gathered in layer 1. The principles address privacy obligations and threats/concerns in the context of managing chronic diseases using mHealth. Some of principles developed in this study address privacy concerns that existing frameworks have not adequately addressed such as invisibility, continuous monitoring and surveillance. A total of 22 privacy principles were developed in the study as shown in Table 3 below.

Framework layer 3 – privacy requirements Privacy requirements (PR) are statements that reference privacy principles and describe the necessary capabilities and functions that are essential for a system to achieve these privacy principles. They are created based on privacy principles in layer 2. When developing privacy requirements, it is necessary to ensure that they are actionable, measurable, testable and traceable. They are also implemented in systems to ensure that the system is compliant with an organisation's privacy policies and principles as well as laws and regulatory frameworks

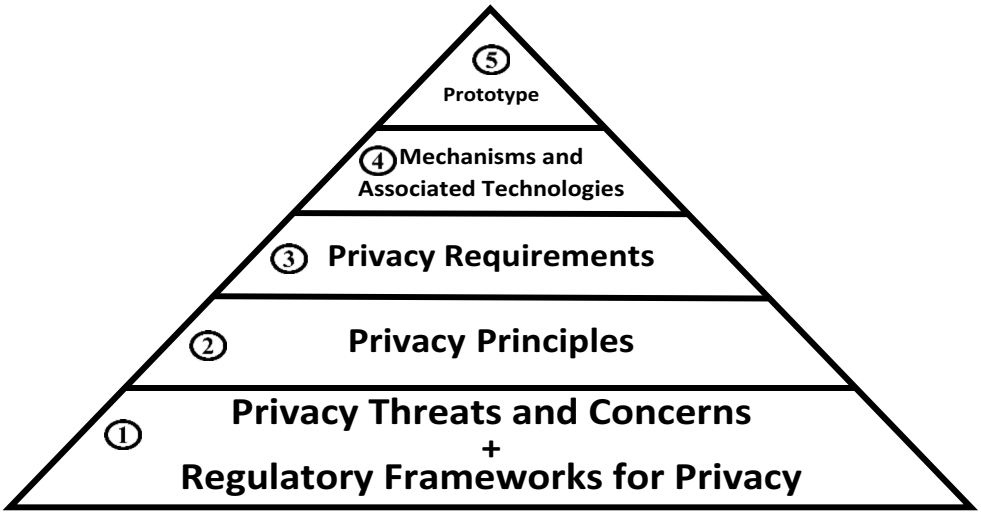

Fig. 2 Proposed privacy framework

(Mitre Corporation 2015). The laws and regulations that govern privacy enunciate privacy requirements at an abstract level which is why it can sometimes prove challenging to developers to interpret and implement them into systems and applications (Mitre Corporation 2013). In this layer, privacy requirements are listed to ensure that privacy principles are addressed and implemented into the design of an mHealth system that implements the proposed framework. The implementation of these privacy requirements will be at the mobile device where data will be processed and at the cloud where data will be stored and accessed by health professionals or third parties such as researchers. In this study, 65 privacy requirements were created based on the privacy principles in layer 2. They are not given in this paper due to the length of the list. However, as an example, for the principle regarding accessibility of data, the following three requirements were created: (i) The system shall allow patients to see what information the system holds about them; (ii) The system shall allow patients to restrict access to their information by third parties; and (iii) The system shall not allow unauthorised access to patient data.

Framework layer 4 – mechanisms and associated technologies The fourth layer of the proposed framework consists of mechanisms and associated technologies that can be used to implement the privacy requirements (given in layer 3). Hence layer 4 is developed based on layer 3. The mechanisms and associated technologies chosen for the purpose of this study include: (i) Access control mechanisms (ACM): to control access to patient data; (ii) Device and storage security (DSs): to enable data to be kept secure for unauthorised use; (iii) Blockchain (Bch): to store patient data as well as implement access control; (iv) Encryption (Enc): to protect patient data during transmission and storage; (v) Anonymisation and pseudo-anonymisation mechanisms (AnP): to allow patient data to be shared with third parties whilst still preserving patient privacy; (vi) System programs (SPr): to implement various system functions. These mechanisms and associated technologies will be used to enable various technical functionalities when developing a prototype to implement the framework and are further discussed below.

Access control mechanisms Access control mechanisms are essential to an mHealth system as they are crucial to ensure that: mHealth data is protected; there are restrictions to access patient data; and vital resources are protected. Access controls are a crucial mechanism which can be used to counter security and privacy threats in mHealth systems. They ensure that access to data is restricted by placing limits on who can access data and therefore only allowing legitimate users to access data. In order to implement an access control mechanism, it is necessary to implement an identification system for both health care practitioners and patients. It is essential that the system is transferable between the various entities that are allowed access to patient data. For the purpose of this study a Role-Based Access Control (RBAC) was chosen. This is appropriate as it will limit data access to third parties such as researchers and allow full access to data for patients and doctors as a means to prevent privacy violations. It can also limit user access based on the user's role within an organisation (Gusmeroli et al. 2013; Rodrigues et al. 2013; Alramadhan and Sha 2017).

Device and storage security mHealth apps and systems face numerous device and storage threats. These include: The susceptibility to privacy threats such as disclosure threats and identity theft; the sharing of data with third parties; and devices storing and transferring unencrypted data. Additional threats include the external devices that mHealth systems utilise to enhance the mHealth system's functionality since these devices may put their users' data at risk as permission systems and protections on mobile platforms do not apply to external

Table 3 Privacy principles developed in layer 2 of the framework

Privacy principle	Explanation of principle
Accessibility of data (P1)	Users have the right to know what information has been collected about them, its purpose, who can access it and where it is being stored and be granted access to their information should they wish to know what data has been collected in regard to them and wish to limit who can access it.
Anonymity (P2)	User's personal identifiable data should be kept anonymous when stored as well as when shared with third parties such as researchers. Users should be identified by a unique identifier known only to the user and their health care practitioner.
Confidentiality (P3)	Appropriate measures need to be put in place in order to ensure doctor–patient confidentiality.
Data control (P4)	Users should have control over the collection, use and access to their data as well as be made aware of how it is being used.
Data quality (P5)	When personal data is collected, it should be reviewed in order to ensure its relevance, accuracy, completeness and that it is up-to-date for the purposes for which it is being used.
Data security (P6)	Adequate protection of personal data should be enforced through security safeguards in order to minimise and protect data from loss, unauthorised access, disclosure and modification. It is also necessary to ensure the confidentiality, integrity and availability of any personal data processed.
Data use (P7)	Personal data should not be used in any manner or form for purposes other than those initially agreed and consented to. User's personal data should only be processed in a lawful manner to ensure that laws and regulations are being complied and adhered to.
Disclosure risks (P8)	Appropriate measures need to be put in place to ensure that users' data is not disclosed, and to inform users if their data is disclosed to an unauthorised party.
Encryption (P9)	Appropriate encryptions methods should be implemented in order to ensure that data cannot be deciphered should it be unlawfully accessed when stored or intercepted whilst being transmitted between devices.
Information misuse/abuse (P10)	The extent to which an individual's information should be collected, used or disclosed should be limited to what the user initially consented to.
Invisibility (P11)	Reminders should be set periodically in order to inform patients of monitoring devices that they use in order to minimise the risk of invisibility.
Profiling (P12)	In order to mitigate profiling, there should not be any storage or analysis of patients psychological, physical and behavioural characteristics, such as the storage of patient frequently visited locations.
Storage limitation (P13)	Personal identifiable data should not be kept for any longer than necessary for its intended purpose or until the data owner requests its deletion.
Sharing of data (P14)	Sharing of data with third parties or researchers should only be allowed if patients have consented to this and should be notified should a third-party request or use their data. The patients should be allowed to see what information on them has been shared.
Surveillance (P15)	Appropriate user controls need to be put in place for users to disable access to certain features of the smartphone which can enable the surveillance of a user. However, this must be done in a way that does not reduce the effectiveness of the monitoring of the disease.
Volume of data collected (P16)	When collecting user data, it is necessary to ensure that the data collected is relevant to a specific purpose. Owing to the large amount of data produced by wearable devices, it is necessary to tailor data presentation to individual patients in order to encourage consistent use.
Continuous monitoring (P17)	Users should be made aware of the continuous monitoring capabilities of their health sensors through a daily reminder. Users should also have the option to disable continuous monitoring and opt for readings during certain intervals or when the devices sense that the user is performing an activity. In the event that the user opts for interval readings, they should be made aware that this will not guarantee the best results for the monitoring and treatment of their condition.
Choice & consent (P18)	It is necessary for consent to be obtained, whether it is implicit or explicit before user data is collected and processed.
Collection limitation (P19)	Data should only be collected if it is relevant and accurate for a particular purpose and should occur only with the knowledge and consent of the user.
Accountability (P20)	The data controller has the responsibility to ensure compliance with all data protection obligations.
Notice (P21)	Appropriate information notices regarding data processing as required by law must be given to patients. Also, other relevant notices should be given to the patient.
Device visibility (P22)	User's wearable devices or sensors should only be identified by its owner and not by any other mobile device in its proximity.

sensors devices (Hussain et al. 2018). Based on the threats mentioned above it is necessary to ensure that mHealth systems and their devices are adequately secure because the data stored and produced are sensitive in nature. In order to ensure adequate device and storage security the Advanced Encryption Standard (AES) to safeguard users' confidentiality of data was chosen. It is a successor to Digital Encryption Standard (DES) which used 56 bits for its key size compared to the 128, 192 or 256-bit key sizes used by AES; therefore, making AES much more secure and harder to decrypt (Robertazzi 2012).

Blockchain The combination of mHealth and blockchain technology provides an effective solution that allows for both data accessibility and transparency. A study done by Ichikawa et al. (2017) showed that blockchain can be utilised as a tamperproof system for mHealth. The Hyperledger Fabric blockchain (an open-source permissioned distributed ledger) was chosen as a suitable blockchain in the context of this study. It will be implemented in a prototype as part of the mHealth system for patient records as well as to create access logs to enable detection of privacy violations. As a private blockchain, it can enable the restriction of who can participate in its network as well as which transactions take place (Pirtle and Ehrenfeld 2018). The benefits of using Hyperledger fabric include: modularity, enabling functionalities to be altered to best suit systems; enabling smart contracts written in java; enabling restricted data access and data confidentiality; and being open-source.

Encryption Data encryption is a mechanism whereby an algorithmic procedure converts user data into a form in which there is a reduced probability of allocating meaning to data without use of a confidential process or key. Encryption can be applied granularly, such as to an individual file containing sensitive information, or broadly, such as encrypting all stored data (Snell 2017). The implementation of encryption is also necessary to comply with data protection regulations, including integrity and confidentiality.

Anonymisation and pseudonymisation mechanisms Anonymisation works by permanently removing personally

Table 4 Mechanisms and associated technologies and the privacy principles they implement

Privacy principles	Mechanisms and associated technologies					
	Access control mechanisms (ACM)	Device and storage security (DSs)	Blockchain (B)	Encryption (E)	Anonymisation and pseudo-anonymisation mechanisms (A)	System programs (SPr)
Accessibility of data (P1)	•		•	•		•
Anonymity (P2)					•	
Confidentiality (P3)	•	•	•	•	•	
Data control (P4)	•	•	•			•
Data quality (P5)						•
Data security (P6)	•	•	•	•		
Data use (P7)			•			•
Disclosure risks (P8)	•	•	•			
Encryption (P9)		•		•		
Information misuse/abuse(P10)	•	•	•			
Invisibility (P11)						•
Profiling (P12)						•
Storage limitation (P13)		•				
Sharing of data (P14)	•		•		•	•
Surveillance (P15)			•			•
Volume of data collected (P16)						•
Continuous monitoring (P17)						•
Choice and consent (P18)						•
Collection limitation (P19)						•
Accountability (P20)	•	•		•	•	
Notice (P21)						•
Device visibility (P22)						•

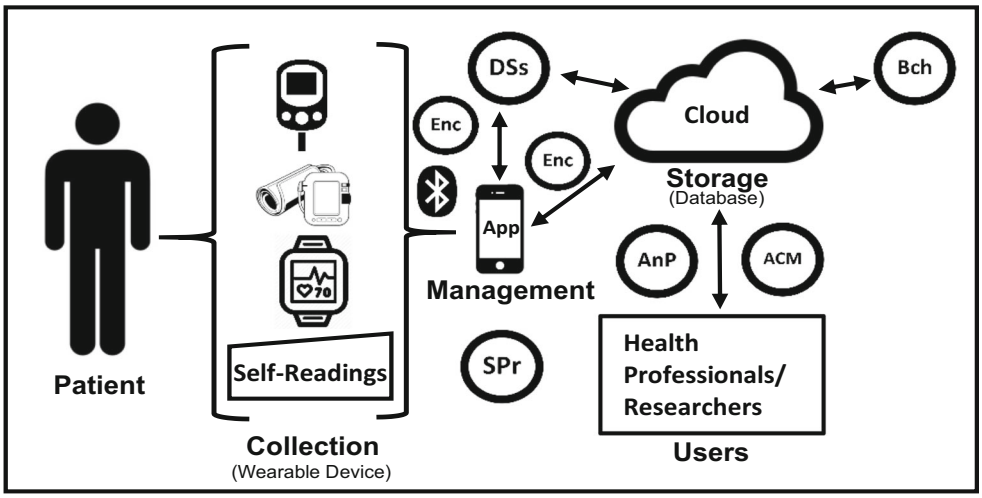

Fig. 3 Prototype implementing the proposed new framework

identifiable data (such as surnames, addresses) from datasets. It allows patient data to be shared (especially with third parties) whilst still preserving patient privacy. Pseudonymisation, however, involves stripping direct identifiers from personal data and substituting them with pseudonyms. This is a reversable process whereby the data can be re-identified if necessary (e.g. by an authorised user such a medical professional). The General Data Protection Regulation (GDPR) mandates the use of pseudonymisation as an appropriate safeguard to reduce risks to data subjects and to enable better compliance with data protection obligations.

System programs System programs perform operations that will ensure that there is appropriate data quality, user opt-in controls to certain system features and the provision of various reminders among other system functions. The system programs will be coded using Java and will be implemented on an SQL database as well as on the mobile application. The system programs chosen for this study facilitate functions such as: remote wipe; consent; data quality; reminders; opt-in controls; system audits; permission controls; data transparency; access logs and audit logs (Table 4).

Table 5 New framework and existing relevant privacy frameworks and the threats/concerns they address

Privacy threats and concerns for mHealth and chronic diseases	Regulatory frameworks for privacy							
	Proposed framework	HPP	Markle	ONC	GAPP	MHHCS	OECD	GDPR
Accessibility of data	•	•	•	•	•	•	•	
Anonymity	•							•
Confidentiality	•	•	•	•		•		
Continuous monitoring	•							
Data control	•	•	•	•		•	•	
Data quality	•		•	•	•	•	•	•
Data security	•	•	•	•	•	•	•	•
Data use	•		•	•	•	•	•	•
Disclosure risks	•	•	•	•	•	•	•	•
Encryption	•							•
Information misuse/abuse	•	•	•	•	•	•	•	•
Invisibility	•							
Profiling	•							•
Sharing of data	•	•	•	•		•	•	•
Surveillance	•							
Volume of data collection	•		•	•	•	•	•	•

Framework layer 5 – prototype The fifth layer of the proposed framework brings together the mechanisms and associated technologies discussed in layer 4 to develop a prototype as illustrated in Fig. 3.

Figure 3 gives an overview of how the mHealth system prototype will implement the proposed framework.

The prototype will be developed to test and evaluate the implementation of the proposed framework in an mHealth system. The prototype consists of mechanisms and associated technologies to implement the privacy requirements specified in the framework. Access control mechanisms (ACM) will be used when stored data is accessed by the users. Device and storage security (DSs) will be used on the mobile device as well as in storage. Blockchain (Bch) will be used when data is stored and accessed. Encryption (Enc) will be used when data is being transmitted from a sensor or wearable to the mobile device and when data is being transmitted to and stored on the cloud. Anonymisation and pseudo-anonymisation mechanisms (AnP) will be used when data is shared with third parties such as researchers. System programs (SPr) will exist throughout the whole mHealth system but will be predominantly found on the mobile device which performs system management.

Comparison of proposed framework to existing frameworks

Table 5 compares the proposed framework to relevant existing privacy frameworks to demonstrate how privacy threats/concerns are addressed. As shown, unlike the new proposed framework, no single existing regulatory frameworks addresses all privacy concerns identified (from existing literature) when managing chronic diseases using mHealth. Furthermore, no existing relevant framework covers some privacy threats and concerns namely: continuous monitoring, invisibility and surveillance.

Conclusion

The high cost of healthcare, limited medical resources and incidences such as the Covid-19 pandemic have highlighted the importance of mHealth as an essential technology to facilitate healthcare at a distance. The increasing global rise of chronic diseases also presents a challenge that can in part be mitigated by the use of mHealth technologies, especially for monitoring, treatment and support. Use of many of these technologies, however, pose potential damage to patients due to privacy infringements. Furthermore, the perceived privacy risks of these technologies may negatively impact trust and adoption intention among patients. The privacy framework developed in this study makes an important contribution to the healthcare domain by directly addressing mHealth privacy threats and concerns identified in previous research. The framework also builds upon existing privacy frameworks but also incorporates new technologies such as blockchain, mechanisms such as encryption and anonymisation, and capabilities such as access controls in order to ensure that data and bodily privacy are addressed. It also allows users to have better control and transparency over how their data is processed, stored and shared. Ongoing work involves the development and evaluation of a functional prototype (layer 5) to fully demonstrate the implementation of the framework. This work hopefully will make a valuable contribution to a post-Covid-19 world, where mHealth technologies will play an integral part in global healthcare, with patient privacy as an integral part of any widespread implementation.

Authors' contributions Equal contribution from all authors.

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

Availability of data and material (data transparency) Not applicable.

Code availability (software application or custom code) Not applicable.

Declarations

Ethical approval Not Applicable.

Informed consent The authors declare that this research does not contain any individual person's data in any form (including any individual details, images or videos).

Consent to participate Not applicable.

Consent for publication Not applicable.

Conflict of interest The authors declare that they have no conflicts of interest.

References

Alramadhan M, Sha K (2017) An overview of access control mechanisms for internet of things. In: 2017 26th international conference on computer communication and networks (ICCCN). IEEE, pp 1–6. https://doi.org/10.1109/ICCCN.2017.8038503

Arora S, Yttri J, Nilse W (2014) Privacy and security in mobile health (mHealth) research. Alcohol Res: Curr Rev 36(1):143–151

Avancha S, Baxi A, Kotz D (2012) Privacy in mobile technology for personal healthcare. ACM Comput Surveys (CSUR) 45:1–54

Brey P (2005) Freedom and privacy in ambient intelligence. Ethics Inf Technol 7:157–166

Brüggemann T, Henson J, Dehling T, Sunyaev A (2016) An information privacy risk index for mHealth apps. In: Schiffner S, Serna J, Ikonomou D, Rannenberg K (eds) Privacy technologies and policy. APF 2016. Lecture notes in computer science, vol 9857. Springer, Cham https://doi.org/10.1007/978-3-319-44760-5_12

Conroy M (2015) Connecting patients to mHealth applications to enhance self-care management. Home Healthcare Now 33(8):437

Dehling T, Gao F, Schneider S, Sunyaev A (2015) Exploring the far side of Mobile health: information security and privacy of mobile health apps on iOS and android. JMIR Mhealth Uhealth 3(1):e8. https://doi.org/10.2196/mhealth.3672

Deng Z, Hong Z, Ren C, Zhang W, Xiang F (2018) What predicts patients' adoption intention toward mHealth services in China: empirical study. JMIR Mhealth Uhealth 6(8):e172. https://doi.org/10.2196/mhealth.9316

Estrin D, Sim I (2010) Open mHealth architecture: an engine for health care innovation. Science 330:759–760

European Commission (2011) Advice paper on special categories of data ("sensitive data"). https://ec.europa.eu/justice/article-29/documentation/other-document/files/2011/2011_04_20_letter_artwp_mme_le_bail_directive_9546ec_annex1_en.pdf. Accessed 15 July 2020

European Commission (2014) Green Paper on mobile Health ("mHealth"). Brussels, 10 April 2014, COM (2014) 219 final. https://ec.europa.eu/digital-single-market/en/news/green-paper-mobile-health-mhealth Accessed 15 July 2020

European Commission (2016) General Data Protection Regulation. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN Accessed 3 April 2020

Guo X, Zhang X, Sun Y (2016) The privacy-personalization paradox in mHealth services acceptance of different age groups. Electron Commer Res Appl 16:55–65

Gusmeroli S, Piccione S, Rotondi D (2013) A capability-based security approach to manage access control in the internet of things, mathematical and computer modelling. Elsevier Ltd 58(5–6):1189–1205. https://doi.org/10.1016/j.mcm.2013.02.006

Harvey MJ, Harvey MG (2014) Privacy and security issues for mobile health platforms. J Assoc Inf Sci Technol 65:1305–1318

Hussain M, Al-Haiqi A, Zaidan A, Bahaa B, Kiah M, Iqbal S, Iqbal SS, Abdulnabi M (2018) A security framework for mHealth apps on android platform, computers & security. Elsevier Ltd 75:191–217. https://doi.org/10.1016/j.cose.2018.02.003

Hutton L, Price BA, Kelly R, McCormick C, Bandara AK, Hatzakis T, Meadows M, Nuseibeh B (2018) Assessing the privacy of mHealth apps for self-tracking: heuristic evaluation approach. JMIR mHealth uHealth 6(10):e185. https://doi.org/10.2196/mhealth.9217

Ichikawa D, Kashiyama M, Ueno T (2017) Tamper-resistant mobile health using blockchain technology, JMIR mHealth and uHealth. JMIR 5(7):e111. https://doi.org/10.2196/mhealth.7938

Iwaya L, Fischer-Hübner S, Åhlfeldt R, Martucci L (2019) Mobile health systems for community-based primary care: identifying controls and mitigating privacy threats. JMIR mHealth and uHealth 7(3):e11642. https://doi.org/10.2196/11642

Jusob F, George C, Mapp G (2017) exploring the need for a suitable privacy framework for mHealth when managing chronic diseases. J Reliable Intell Environ 3(4):243–256

Khandani S (2005) Engineering design process. https://resources.saylor.org/wwwresources/archived/site/wp-content/uploads/2012/09/ME101-4.1-Engineering-Design-Process.pdf. Accessed 20 June 2020

Kotz D, Avancha S and Baxi A (2009) A privacy framework for mobile health and home-care systems. ACM 43(1). https://doi.org/10.1145/1655084.1655086

Markle Foundation (2008) Common framework for networked personal health information: overview and principles. Connecting For Health, June 2008. https://www.markle.org/sites/default/files/Overview.pdf Accessed April 2020

McCarthy M (2013) Experts warn on data security in health and fitness apps. Br Med J 347(1):f5600. https://doi.org/10.1136/bmj.f5600

Mitre Corporation (2013) Privacy requirements definition and testing in the healthcare environment. https://www.mitre.org/sites/default/files/publications/13-2766.pdf. Accessed 14 May 2020

Mitre Corporation (2015) Privacy requirements definition and testing. https://www.mitre.org/publications/systems-engineering-guide/enterprise-engineering/engineering-informationintensive. Accessed 14 May 2020

ONC (2008) Nationwide privacy and security framework for electronic exchange of individually identifiable health information. https://www.healthit.gov/sites/default/files/nationwide-ps-framework-5.pdf. Accessed 07 April 2020

OECD (2013) OECD privacy principles. https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf. Accessed 03 April 2020

Pirtle C, Ehrenfeld J (2018) Blockchain for healthcare: the next generation of medical records? J Med Syst 172(42):1–3

Prosch M (2008) Protecting personal information using generally accepted privacy principles (GAPP) and continuous control monitoring to enhance corporate governance. Int J Discl Gov 5:153–166

Raimundas M (2017) Fundamentals of secure system modelling. Springer, New York, pp 43–60

Robertazzi T (2012) Advanced encryption standard (AES). In: Basics of computer networking. Springer, New York, pp 73–77. https://doi.org/10.1007/978-1-4614-2104-7_10

Rockwell K, Gilroy A (2020) Incorporating telemedicine as part of COVID-19 outbreak response systems. Am J Manag Care 26(4):147–148. https://doi.org/10.37765/ajmc.2020.42784

Rodrigues et al (2013) Analysis of the security and privacy requirements of cloud-based electronic health records systems. J Med Internet Res 15(8):e186–e186. https://doi.org/10.2196/jmir.2494

Shilton K (2009) Four billion little brothers? Privacy, mobile phones, and ubiquitous data collection. ACM, New York

Snell E (2017) The difference between healthcare data encryption, de-identification. https://healthitsecurity.com/features/the-difference-between-healthcare-data-encryption-de-identification. Accessed 16 June 2020

Steinhubl S, Muse E and Topol E (2015) The emerging field of mobile health. Sci Transl Med 7(283):283rv3. https://doi.org/10.1126/scitranslmed.aaa3487

Watkins J, Goudge J, Gómez-Olivé X, Huxley C, Dodd K, Griffith F (2018) mHealth text and voice communication for monitoring people with chronic diseases in low-resource settings: a realist review. BMJ Glob Health 3(2):e000543

World Health Organization (2017) Facts sheets: noncommunicable diseases. World Health Organization, Geneva, June 2017. https://wwweurowhoint/__data/assets/pdf_file/0007/350278/Fact-sheet-SDG-NCD-FINAL-25-10-17pdf Accessed 25 March 2021

Yi J, Kim Y, Cho Y, Kim H (2018) Self-management of chronic conditions using mHealth interventions in Korea: a systematic review. Healthcare Inform Res 24(3):187

Zhang X, Guo X, Guo F (2014) Lai KH (2014) nonlinearities in personalization-privacy paradox in mHealth adoption: the mediating role of perceived usefulness and attitude. Technol Health Care 22(4):515–529